## Table of Contents

### Data Center Security Policy Best Practices Checklist
- Plan Your Data Center Best Practice Deployment.......................................................... 7
- Deploy Data Center Best Practices.................................................................................. 9
- Follow Post-Deployment Data Center Best Practices...................................................... 18

### Data Center Best Practice Security Policy
- What Is a Data Center Best Practice Security Policy?...................................................... 21
- Why Do I Need a Data Center Best Practice Security Policy?.......................................... 22
- Data Center Best Practice Methodology.......................................................................... 23
- How Do I Deploy a Data Center Best Practice Security Policy?........................................ 26
- How to Assess Your Data Center....................................................................................... 27
- How to Decrypt Data Center Traffic................................................................................ 30
  - Create the Data Center Best Practice Decryption Profiles............................................ 31
  - Exclude Unsuitable Traffic from Data Center Decryption.............................................. 36
- Create a Data Center Segmentation Strategy................................................................. 37
  - How to Segment the Data Center ................................................................................. 37
  - How to Segment Data Center Applications................................................................. 38
- How to Create Data Center Best Practice Security Profiles........................................... 41
  - Create the Data Center Best Practice Antivirus Profile............................................... 41
  - Create the Data Center Best Practice Anti-Spyware Profile......................................... 42
  - Create the Data Center Best Practice Vulnerability Protection Profile........................ 44
  - Create the Data Center Best Practice File Blocking Profile........................................ 45
  - Create the Data Center Best Practice WildFire Analysis Profile.................................. 46
- Use Traps to Protect Data Center Endpoints................................................................. 48
- Create Data Center Traffic Block Rules.......................................................................... 49
- Define the Initial User-to-Data-Center Traffic Security Policy....................................... 53
  - User-to-Data-Center Traffic Security Approaches......................................................... 53
  - Create User-to-Data-Center Application Whitelist Rules.............................................. 54
  - Create User-to-Data-Center Authentication Policy Rules............................................. 58
  - Create User-to-Data-Center Decryption Policy Rules.................................................... 60
- Define the Initial Internet-to-Data-Center Traffic Security Policy................................. 64
  - Internet-to-Data-Center Traffic Security Approach....................................................... 64
  - Create Internet-to-Data-Center Application Whitelist Rules....................................... 65
  - Create Internet-to-Data-Center Decryption Policy Rules............................................. 66
  - Create Internet-to-Data-Center DoS Protection Policy Rules......................................... 67
- Define the Initial Data-Center-to-Internet Traffic Security Policy..................................... 69
  - Data-Center-to-Internet Traffic Security Approaches.................................................... 69
  - Create Data-Center-to-Internet Application Whitelist Rules......................................... 70
  - Create Data-Center-to-Internet Decryption Policy Rules............................................... 74
- Define the Initial Intra-Data-Center Traffic Security Policy........................................... 76
  - Intra-Data-Center Traffic Security Approach................................................................ 76
  - Create Intra-Data-Center Application Whitelist Rules................................................. 77
  - Create Intra-Data-Center Decryption Policy Rules......................................................... 80
- Order the Data Center Security Policy Rulebase............................................................ 81
- Log and Monitor Data Center Traffic.............................................................................. 84
  - What Data Center Traffic to Log and Monitor.............................................................. 84
  - Monitor Data Center Block Rules and Tune the Rulebase............................................ 86
- Log Intra Data Center Traffic That Matches the Intrazone Allow Rule........................... 87
- Log Data Center Traffic That Matches No Interzone Rules............................................ 89
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain the Data Center Best Practice Rulebase</td>
<td>91</td>
</tr>
<tr>
<td>Use Palo Alto Networks Assessment and Review Tools</td>
<td>93</td>
</tr>
</tbody>
</table>
Data Center Security Policy Best Practices Checklist

Your enterprise’s most valuable assets reside in your data center, including proprietary source code, intellectual property, and sensitive company and customer data. Your customers and employees trust you to maintain the confidentiality and integrity of their data and expect that data to be always available, so it’s important to implement a data center best practice security policy that safeguards your data and prevents successful attacks. It’s not enough to harden the network perimeter because attacks can originate from inside the network, attacks can come from partners and contractors whose credentials have been compromised, and because if an attacker gains a foothold in your network, the attacker can attack from the inside of the network by moving laterally from device to device.

If you are familiar with Palo Alto Networks platform, you can save time by using this streamlined checklist to implement pre-deployment, deployment, and post-deployment data center security policy best practices. Each section includes links to detailed information in the full Data Center Best Practice Security Policy document or in the PAN-OS 9.0 Admin Guide, including how to configure policy rules and security profiles.

> Plan Your Data Center Best Practice Deployment
> Deploy Data Center Best Practices
> Follow Post-Deployment Data Center Best Practices
Plan Your Data Center Best Practice Deployment

Prepare to implement best practices in your data center by developing a strategy and a roll-out plan. Use positive security enforcement (create rules that allow the user and application traffic you want to allow and deny everything else, also known as whitelisting) to work toward a Zero Trust architecture.

**STEP 1 | Set goals.**

- Define the ideal future state of your data center network so you have definitive goals to work toward and know when you’ve achieved those goals.
- Protect traffic flows from each area in which connections are initiated:
  1. Local user traffic flowing into the data center.
  2. Traffic flowing from the internet to the data center.
  3. Traffic flowing from the data center to the internet.
  4. Traffic flowing between servers or VMs within the data center (intra data center east-west traffic).
- Don’t allow unknown users, applications, or traffic in your data center.
- Create a standardized, scalable design you can replicate and apply consistently across data centers.

**STEP 2 | Work with stakeholders such as IT/support, security, and groups that require data center access such as engineering, legal, finance, and HR, to develop an access strategy.**

- Identify users who need access, and the assets to which they need access. Understanding this enables you to create user groups based on access level requirements so you can design efficient Security policy rules by user group.
- Identify the applications you want to allow (sanction) in the data center. To reduce the attack surface, only sanction applications for legitimate business reasons.

**STEP 3 | Assess your data center to understand its current state so you can create a plan to transform data center security to the desired future state.**

- Inventory the physical and virtual environment and assets, including:
  - Servers, routers, switches, security devices, load balancers, and other network infrastructure.
  - Standard and proprietary custom applications and the service accounts they use to communicate. Compare the application inventory list to the list of applications you want to sanction.

  _Focus on the applications you want to allow because your whitelist Security policy rules allow them and by default deny all other applications to reduce the attack surface. Map applications to business requirements. If an application doesn’t map to a business requirement, evaluate whether you really need to allow it._

- Assess each asset to help prioritize what to protect first. Ask yourself questions such as, “What defines and differentiates our company?”, “What systems must be available for daily operations?”, and “If I lost this asset, what are the consequences?”
- Work with application, network, and enterprise architects, and with business representatives to characterize data center traffic flows and learn about typical baseline traffic loads and patterns so you understand normal network behavior. Use the Application Command Center widgets and traffic analysis tools to baseline traffic.

**STEP 4 | Create a Data Center Segmentation Strategy to prevent malware that gains a foothold in your data center from moving laterally to infect other systems.**
Use firewalls as segmentation gateways to provide visibility into data center traffic and systems so you can finely control who can use which applications to access which devices. Segment and secure non-virtualized servers with physical firewalls and the virtual network with VM-Series firewalls.

- Use the firewall's flexible segmentation tools such as zones, dynamic address groups, App-ID, and User-ID to design a granular segmentation strategy that protects sensitive servers and data.
- Group assets that perform similar functions and require the same level of security in the same segment.
- Segment data center applications by segmenting the server tiers that make up an application tier (typically a service chain composed of a web server tier, an application server tier, and a database server tier) and using the firewall to control and inspect traffic between tiers.
- Consider using an SDN solution inside the data center for an agile, virtualized infrastructure that maximizes resource utilization and makes automation and scaling easier.

**STEP 5** | Plan to use best practice methodology to inspect all data center traffic and gain complete visibility, reduce the attack surface, and prevent known and unknown threats.

- Position physical or virtual firewalls where they can see all data center network traffic.
- Take advantage of the firewall's powerful toolset to create application-based Security policy rules tied to specific user groups and protected by Security profiles. Forward unknown files to WildFire and deploy decryption to prevent threats from entering the data center in encrypted traffic.
- Use GlobalProtect in internal mode as a gateway to control data center access.
- Authenticate users to prevent unauthorized access and configure Multi-Factor Authentication for access to sensitive applications, services, and servers, especially by contractors, partners, and other third-parties who require access to your data center.
- Manage firewalls centrally with Panorama to enforce consistent policy across physical and virtual environments and for centralized visibility.
- If you have multiple data centers, reuse templates and template stacks to apply consistent security policy across different locations.

**STEP 6** | Phase in your best practice deployment over time; start by focusing on the most likely threats to your business and network, and protect your most valuable assets first.

Taking into account all of the data center users, applications, devices, and traffic flows, and then creating best practice Security policy around them may seem like an overwhelming task if you try to do everything at one time. But by protecting your most valuable assets first and planning a phased, gradual implementation, you can transition in a smooth and practical way from a hope-for-the-best Security policy to a best practice Security policy that safely enables applications, users, and content.
Deploy Data Center Best Practices


For Security, Authentication, and DoS policy rules, configure log forwarding to Panorama or external services to centralize logs for convenient viewing and analysis, with notifications.

STEP 1 | If your data center application inventory includes proprietary custom applications, then create custom applications for them so that you can specify them in Security policy.

STEP 2 | Configure tight data center best practice Security profiles to prevent threats from disrupting your data center network.

- Configure the best practice Antivirus profile by cloning the predefined profile and changing the imap, pop3, and smtp decoder values to `reset-both` in the Action and WildFire Action columns.
- Configure the best practice Anti-Spyware profile by cloning the predefined strict profile. On the Rules tab, enable single packet capture on medium, high, and critical severity threats for traffic you log. (For traffic you don’t log, apply a separate profile without packet capture enabled.)

On the DNS Signatures tab, change the Action on DNS Queries to `sinkhole` if the firewall can’t see the originator of the DNS query (typically when the firewall is north of the local DNS server) so that you can identify infected hosts. DNS sinkhole identifies and tracks potentially compromised hosts that attempt to access suspicious domains and prevents them from accessing those domains. Enable extended packet capture on the sinkholed traffic.

- Configure the best practice Vulnerability Protection profile by cloning the predefined strict profile and changing the Packet Capture setting for every rule except `simple-client-informational` and `simple-server-informational` to `single-packet`. If the firewall identifies a large volume of vulnerability threats and that affects performance, disable packet capture for low-severity events.
- The predefined strict File Blocking profile is the best practice profile. If supporting critical applications prevents you from blocking all the file types the strict profile blocks (you can identify the file types used in the data center from data filtering logs at Monitor > Logs > Data Filtering), clone the strict profile and modify it as needed. If files don’t need to flow in both directions, use the Direction setting to restrict the file type to only the required direction.

- The predefined WildFire Analysis profile is the best practice profile. WildFire provides the best defense against unknown threats and advanced persistent threats (ATPs).

STEP 3 | Configure tight data center best practice Decryption profiles to prevent unknown traffic from entering your data center.

- Perform CRL/OCSP checks to ensure that certificates presented during SSL decryption are valid.
- SSL Protocol Settings: Set the Min Version to TLSv1.2, the Max Version to Max, and uncheck the SHA1 Authentication Algorithm. (The weak 3DES and RC4 Encryption Algorithms are automatically unchecked when you select TLSv1.2.)
- SSL Forward Proxy: For Server Certificate Verification, block sessions with expired certificates, untrusted issuers, and unknown certificate status, and restrict certificate extensions. For Unsupported Mode Checks, block sessions with unsupported versions, unsupported cipher suites, and client authentication. For Failure Checks, blocking sessions if resources aren’t available is a tradeoff between the user experience (blocking may negatively affect the user experience) and potentially allowing dangerous connections. If you have to consider this tradeoff, also consider increasing the decryption resources available in the deployment.
- SSL Inbound Inspection: For Unsupported Mode Checks, block sessions with unsupported versions and unsupported ciphers. For Failure Checks, the tradeoffs are similar to SSL Forward Proxy.
- SSH Proxy: For **Unsupported Mode Checks**, block sessions with unsupported versions and unsupported algorithms. For **Failure Checks**, the tradeoffs are similar to SSL Forward Proxy.
- Apply the **No Decryption** profile to traffic you choose not to decrypt because of regulations, compliance rules, or business reasons. Block sessions with expired certificates and untrusted issuers.

**STEP 4 | Configure traffic blocking rules** to deny traffic you know is malicious or isn’t needed for business purposes.

Logging and monitoring block rules may reveal users and applications you didn’t know were on your network and that may be legitimate or may indicate an attack. The rule order in the Security policy rulebase is critical to prevent *shadowing* (traffic matching an allow or block rule before it can match the rule you intend the traffic to match). Some rules are almost the same but enable separate reporting for standard and non-standard ports or for user applications and applications from other sources. For each rule, configure **Log at Session End** on the Actions tab and set up **Log Forwarding** to track and analyze rule violations.

- Block all applications from user zones on the **application-default** port. Place this rule *after* the rules that allow legitimate application traffic from user zones to identify unknown or unexpected user applications on standard ports.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>User to DC</td>
<td>any</td>
<td>Web-Server-Tier DC</td>
<td>Drop</td>
</tr>
</tbody>
</table>

- Block all applications from user zones on **any** port to catch user traffic attempting to use non-standard ports. Place this rule after the preceding **application-default** block rule to identify unknown or unexpected user applications on non-standard ports, which may be custom applications or evasive applications.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>User to DC</td>
<td>any</td>
<td>Web-Server-Tier DC</td>
<td>Drop</td>
</tr>
</tbody>
</table>

- Blacklist applications you *never* want in your data center, such as evasive and commonly exploited applications and applications not required for business. Place this rule after the application whitelist rules so that, for example, you allow sanctioned file sharing applications before the **Filesharing-Appfilter** blocks all other file sharing applications.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

- Block all applications from **any** zone on the **application-default** port to identify unexpected applications on standard ports. Rule matches may indicate potential threats or application changes.
that require modifying a whitelist rule. Place this rule after the application whitelist rules and the preceding block rule.

- Block all applications from any zone on any port to identify unexpected applications on non-standard ports. Don’t allow unknown-tcp, unknown-udp, or non-syn-tcp traffic. Place this rule after the application whitelist rules and the preceding block rule.

- Block unknown users attempting to run applications on any port to discover unknown users (gaps in User-ID coverage or attackers) and identify compromised devices (including embedded devices such as printers, card readers, and cameras). Place this rule after the application whitelist rules and the preceding block rule.

**STEP 5** | Create application whitelist Security policy rules for user traffic to allow appropriate access.

Place whitelist rules for user access at the top of the rulebase, before block rules, to prevent accidentally blocking legitimate traffic. For each rule, configure Log at Session End on the Actions tab and set up Log Forwarding to track and analyze rule violations.

- Enable employee user access to internal corporate DNS servers. This rule allows any user because users access DNS services before they log in. The rule tightly controls the source zone, destination servers, and application, and applies Security profiles to the traffic.

  Block access to external DNS servers at the internet gateway to prevent DNS traffic from going out on the internet to public servers.

- Allow secured, privileged access to data center management interfaces for the necessary IT personnel. Restrict the rule to management interfaces (this example uses an address group to identify the devices and a custom service to identify the management ports) and the necessary applications, in this example, RDP, SSH, and SSL. Use a dedicated VLAN to separate management traffic from other traffic and place management interfaces on the same subnet.

  If the same IT user group also manages switches, routers, and other data center devices, add them to the destination and add their ports to the custom service so the rule secures traffic for connections to their management interfaces. If different IT groups manage different data center resources, create separate Security policy rules and corresponding Decryption and Authentication policy rules for each group.
Allow required access for employee user groups. These rules limit each user group's (or user's) access to the necessary applications and servers. This example limits an engineering user group's access to only its development servers and applications.

Allow targeted, limited access to contractors, partners, customers, and other third-parties. This example limits access for an SAP contractor group so the group can reach only the appropriate SAP database servers, using only the appropriate applications.

**STEP 6** Create Authentication policy rules for user traffic to authenticate data center access.

For each user group or user for whom you create application whitelist rules, create an analogous authentication rule (except the DNS whitelist rule because DNS occurs before users authenticate to log in). For each rule, configure **Log at Session End** on the **Actions** tab and set up Log Forwarding to track and analyze rule violations.

Authenticate users who need specialized access. This example authenticates the IT personnel who need secure privileged access to manage data center servers from the preceding step's whitelist rule. Because compromising the credentials of a privileged user hands an attacker the keys to your data center kingdom, require **Multi-Factor Authentication** (MFA) to protect against stolen credentials.

If the same IT user group also manages switches, routers, and other data center devices, add them to the destination and add their ports to the custom service so the rule authenticates traffic for connections to their management interfaces. If different IT groups manage different data center resources, create separate Security policy rules and corresponding Decryption and Authentication policy rules for each group.

Authenticate employees with legitimate business reasons to access the data center. This example authenticates the engineering development user group from the preceding step's whitelist rule.

Authenticate contractors, partners, customers, and other non-employee groups. Require MFA for non-employee groups to protect against credential theft at a third-party company. This example authenticates the SAP developers from the preceding step's whitelist rule.
STEP 7 | Create Decryption policy rules for user traffic to decrypt traffic you allow so the firewall can see, inspect, and apply Security policy to the traffic.

For each Decryption policy rule, apply the appropriate best practice Decryption profile (SSL Inbound Inspection, SSL Forward Proxy, SSH Proxy, or No Decryption, including best practice SSL Protocol Settings for SSL Inbound Inspection and SSL Forward Proxy rules) to block weak protocols and algorithms and to verify server certificates. For each SSL Inbound Inspection rule, import the certificate of the of the data center server you are protecting with decryption.

Exclude traffic from decryption only for these two reasons:

- Traffic breaks decryption for technical reasons, such as a pinned certificate or mutual authentication. Add technical exclusions to the Device > Certificate Management > SSL Decryption Exclusion list.
- Traffic that you choose not to decrypt because of business, regulatory, compliance, or other reasons, such as financial, health, or government traffic. Create policy-based decryption exclusions for traffic you choose not to decrypt.

Decrypt traffic from the previously created Security policy rule that allows IT privileged access to management servers. The Decryption policy rule and its associated Decryption profile differ depending on whether the IT group uses SSL (SSL Forward Proxy Decryption profile) or SSH (SSH Proxy Decryption profile) to access management ports.

If the same IT user group also manages data center switches, routers, and other devices, add them to the destination and add the server certificates so the rule decrypts traffic for connections to their management interfaces. If different IT groups manage different sets of data center resources, create separate, tight Security policy rules and corresponding Decryption and Authentication policy rules for each group.

For SSL privileged access:

For SSH privileged access:

Configure SSL Inbound Inspection to decrypt allowed traffic from employee user groups. This example decrypts traffic from the analogous engineering development user group whitelist rule.

Configure SSL Inbound Inspection to decrypt allowed traffic from contractors, partners, customers, and other third-parties. This example decrypts traffic from the analogous SAP contractor user group whitelist rule.
Apply a No Decryption profile to configure server verification for traffic that you choose not to decrypt because of business, regulatory, compliance, or other reasons, such as financial, health, or government traffic. This example shows how to exclude two groups of finance users from decryption when they access servers in the Fin Servers address group.

**STEP 8** | Create application whitelist Security policy rules for internet-to-data-center traffic to control and secure partner, contractor, and customer access.

Protect against downloading malware from an infected external client or placing malware on an external server from an infected data center server. Whitelist applications required for business purposes and create an External Dynamic List (EDL) to block bad IP addresses. For each rule, configure Log at Session End on the Actions tab and set up Log Forwarding to track and analyze rule violations.

This example restricts the applications and destinations for internet-to-data-center traffic, and uses the Negate option to prevent communication with the Bad IPs List EDL.

Create similar rules for traffic from the internet to other server groups (if allowed) and other applications. Make each rule specific to limit access to only the required applications and servers.

**STEP 9** | Create Decryption policy rules for internet-to-data-center traffic to decrypt allowed traffic.

Configure SSL Inbound Inspection (and import the destination server certificates into the firewall) to decrypt partner, contractor, and customer traffic that Security policy rules allow for internet-to-data-center traffic. This example shows the Decryption policy for the preceding Security policy rule.

Create Decryption rules to match traffic that internet-to-data-center Security policy rules allow.

**STEP 10** | Create internet-to-data-center DoS Protection policy rules to protect sensitive servers from Denial-of-Service (DoS) attacks by limiting the number of connections-per-second (CPS) the firewall allows to the servers to prevent a SYN flood attack.

Attackers target the web server tier because if they take it down, they prevent most legitimate access to the data center. Apply a classified DoS Protection policy rule with a DoS Protection profile that limits the incoming CPS to prevent traffic spikes that can affect server performance and availability.

Create a classified DoS Protection profile to protect the web server tier and prevent SYN flood attacks. The CPS thresholds you set depend on the baseline peak CPS rate.
Create a DoS Protection policy rule to specify the web servers you’re protecting and apply the classified DoS Protection profile to it.

To protect against SYN flood attacks from internal sources, create a separate DoS Protection policy rule that specifies your internal zones as the source zone instead of **L3-External**. Separate rules for external and internal attack sources provides separate reporting that makes investigating attack attempts easier.

To protect against single-session DoS attacks, configure Packet Buffer Protection for each data center zone to protect the firewall from legitimate traffic to drop.

**STEP 11** Create **data-center-to-internet** whitelist rules to protect connections to external servers.

Data center servers may obtain software updates or certificate status from servers on the internet. The greatest risk is connecting to the wrong server. Create strict whitelist rules for updates to limit the reachable external servers and the allowed applications (on default ports only). This prevents infected data center servers from phoning home and prevents data exfiltration using legitimate applications such as FTP, HTTP, or DNS on non-standard ports. In addition, use the File Blocking profile’s **Direction** control to block outbound update files so you only allow downloading for software update files.

For each rule, apply best practice Security profiles and configure **Log at Session End** on the **Actions** tab.

*Work with engineering and other groups that update software to log and analyze web browsing sessions to define the URLs to which developers connect for updates.*

These examples allow engineering servers to communicate with CentOS update servers (**CentOS-Update-Servers** custom URL Category) using the **yum** application and with Microsoft update servers (**Win-Update-Servers** custom URL Category) using the **ms-update** application (you must also allow **ssl** because **ms-update** has a dependency on **SSL**).
Allow access to DNS and NTP updates (\textit{NTP DNS Update Servers custom URL Category}).

Allow connecting to an internet Online Certificate Status Protocol (OCSP) Responder to check the revocation status of authentication certificates and ensure they are valid. When you configure a certificate profile on the firewall, set up CRL status verification as a fallback method for OCSP in case the OCSP Responder is unreachable.

STEP 12 | Create data-center-to-internet Decryption policy rules to decrypt the traffic allowed in the preceding Security policy rules.

A compromised update server could download malware and propagate it through the software update process, so decrypting traffic to gain visibility is critical. Because only service accounts initiate update traffic and update traffic has no personal or sensitive information, there are no privacy issues.

\textit{Don't decrypt traffic to OCSP certificate revocation servers because the traffic usually uses HTTP, so it's not encrypted. In addition, SSL Forward Proxy decryption may break the update process because the firewall acts as a proxy and replaces the client certificate with a proxy certificate, which the OCSP responder may not accept as valid.}

Decrypt traffic between data center and update servers. These two examples decrypt the CentOS and Windows update traffic allowed by the analogous Security policy rules in the preceding step.

Decrypt traffic between data center servers and NTP and DNS update servers. This example decrypts the update traffic allowed by the analogous Security policy rule in the preceding step.

STEP 13 | Create intra-data-center application whitelist rules to protect data center servers from other data center servers that may be compromised.

A common application architecture consists of three server tiers: web servers, application servers, and database servers. Apply best practice Security profiles to most traffic between server tiers to prevent threats. Don't apply Security profiles to low-value, high-volume traffic such as mailbox replication and backup flows—the firewall already inspected the original flows, so spending CPU cycles on them provides no extra value. Do create whitelist access rules for these applications to prevent misuse. For
each rule, configure Log at Session End on the Actions tab and set up Log Forwarding to track and analyze rule violations.

This example configures rules that allow traffic between application server tiers for two proprietary internal finance applications for which we created custom applications: Billing-App and Payment-App.

- Allow finance application traffic between the web server tier and the application server tier.

- Allow finance application traffic between the application server tier and the database server tier.

**STEP 14 |** Arrange the Security policy rules in the correct order so no rule shadows another rule and you allow only the applications you want to allow.

Order the Data Center Security policy rulebase shows the full rulebase from the previous examples (whitelist and blocking rules) in the correct order and explains each rule’s placement.

**STEP 15 |** Install Traps on all data center endpoints to protect against malware and exploits on the endpoints.

Traps protects all endpoints the same way, so the recommended Traps deployment process and malware protection policy best practices are the same for the data center as for any other network area.
Follow Post-Deployment Data Center Best Practices

After you begin deploying data center best practices, monitor the network to ensure that security and access are working as expected, and then maintain the rulebase as circumstances change.

STEP 1 | Check the predefined Applications report (Monitor > Reports > Application Reports > Applications) to verify that only applications you whitelisted in Security policy rules are running.

If you find unexpected applications, review the Security policy rules and refine them to eliminate unexpected applications or to accommodate legitimate applications.

STEP 2 | Log all data center traffic.

Use Palo Alto Networks’ extensive monitoring tools, logging tools, predefined reports, and custom reports to capture and monitor activity for unexpected applications, users, traffic, and behaviors.

STEP 3 | Create custom reports to monitor the block rules, which protect against potential attacks and also identify policy gaps and unexpected behaviors so you can tune the rulebase.

STEP 4 | Create a custom report to log intra-data-center traffic that matches the predefined intrazone-default allow rule at the bottom of the rulebase, which allows all traffic within the same zone by default.

STEP 5 | Enable logging on and create a custom report for data center traffic that matches the predefined interzone-default rule at the bottom of the rulebase, which denies all traffic between zones by default.

STEP 6 | Listen and respond to user feedback.

User complaints about losing access to applications identifies gaps in the rulebase or risky applications that were in use on your network before application whitelisting prevented their use.

STEP 7 | Periodically compare the baseline measurements you took during the planning stage to the current measurements to evaluate progress, identify changes, and find areas of improvement.

At the same time, revisit your goal for the ideal future state of the network to assess progress. If you manage firewalls with Panorama, monitor firewall health to compare devices to their baseline performance and to each other to identify deviations from normal behavior.

STEP 8 | Evolve application whitelist rules over time because applications evolve, user requirements change, and content updates modify existing App-IDs and introduce new App-IDs.

Maintain the data center best practice rulebase and review new and modified App-IDs before you install a new content release so you can modify the rulebase if the changes impact policy.

STEP 9 | Use Palo Alto Networks assessment and review tools to assess your current prevention posture and your adoption of best practices.

STEP 10 | Refer to the full Data Center Best Practice Security Policy for details about each planning, deployment, and post-deployment step and how they benefit you.
Data Center Best Practice Security Policy

Your enterprise’s most valuable assets reside in your data center, including proprietary source code, intellectual property, and sensitive company and customer data. Your customers and employees trust you to maintain the confidentiality of their sensitive data and expect your data center to be always available because they expect their data to be always available. It’s important for the integrity and success of your business to implement a data center best practice security policy that safeguards your data and prevents successful attacks.

The following methods and recommendations provide a blueprint for planning, designing, and implementing a data center best practice security policy in a phased, prioritized manner. Creating a data center best practice security policy may be a daunting task if you try to implement every protection on every area of your network at one time. However, if you evaluate what is most important to protect and begin implementing your data center best practice security policy by defending your most valuable assets first, you can transition gradually to a security policy that allows you to safely enable applications, users, and content without taking undue risks.

The Data Center Security Policy Best Practices Checklist provides an overview of pre-deployment, deployment, and post-deployment best practices, and a way to implement best practices more quickly if you don’t need detailed explanations.

> What Is a Data Center Best Practice Security Policy?
> Why Do I Need a Data Center Best Practice Security Policy?
> Data Center Best Practice Methodology
> How Do I Deploy a Data Center Best Practice Security Policy?
> How to Assess Your Data Center
> How to Decrypt Data Center Traffic
> Create a Data Center Segmentation Strategy
> How to Create Data Center Best Practice Security Profiles
> Use Traps to Protect Data Center Endpoints
> Create Data Center Traffic Block Rules
> Define the Initial User-to-Data-Center Traffic Security Policy
> Define the Initial Internet-to-Data-Center Traffic Security Policy
> Define the Initial Data-Center-to-Internet Traffic Security Policy
> Define the Initial Intra-Data-Center Traffic Security Policy
> Order the Data Center Security Policy Rulebase
> Log and Monitor Data Center Traffic
> Maintain the Data Center Best Practice Rulebase
> Use Palo Alto Networks Assessment and Review Tools
What Is a Data Center Best Practice Security Policy?

A data center best practice security policy protects your own company’s valuable data, protects the confidentiality of your customers, partners, and vendors, protects the integrity of your network and business operations as a whole, and helps ensure the constant availability of the network. It protects against attacks that originate outside or inside the network, along all attack vectors.

A data center best practice security policy protects four traffic flows (areas from which connections are initiated):

1. Local user traffic flowing into the data center.
2. Traffic flowing from the internet to the data center.
3. Traffic flowing from the data center to the internet.
4. Intra data center traffic flowing between servers or VMs, also known as east-west traffic.

A data center best practice security policy prevents attackers from gaining a foothold in your data center and prevents any attacker who manages to breach the data center from exfiltrating data or moving laterally within the network to compromise critical servers. It prevents both known and unknown threats by implementing security policy rules to achieve best-practice goals that are aligned with your business requirements. It:

- Identifies applications regardless of port, protocol, or evasive technique, including by decrypting encrypted traffic.
- Identifies and controls users regardless of IP address, location, or device.
- Protects against known and unknown application-borne threats and vulnerabilities.
- Detects abnormal behavior that may indicate an attack is in progress.

A data center best practice security policy also catches intruders when they violate a policy rule. Violating a rule stops the attack because the violation causes the next-generation firewall to deny access and logs the violation so you can investigate the issue and take appropriate action.
Why Do I Need a Data Center Best Practice Security Policy?

Protecting the availability, confidentiality, and integrity of your network so that you can run your business securely, without interruption, and in compliance with regulations governing the protection of sensitive data, is critical. The idea that hardening the exterior of the network and allowing the interior of the network to remain soft because the interior is trusted is outdated, leaves the network open to attack from the inside, and doesn’t plan for a scenario in which a determined, resourced, persistent attacker finds a foothold inside the perimeter. That’s why you need to protect the data center perimeter and interior as strongly as you protect the enterprise network perimeter.

Inside attacks can originate from sources such as current employees or on-site contractors. The common thread in inside attacks is that the attack comes from a legitimate user or application source. Outside attacks can originate from cyber-criminals, hacktivists, and state-sponsored attackers, and from less obvious avenues of attack such as compromised partner or vendor systems, or a former employee who knows the network. The first step for an outside attacker is to gain a foothold inside the network, transforming the attack to an inside attack. In essence, all breaches are inside attacks even if they originate on the outside, because once an attacker gains access to the network, the attacker can roam throughout the network.

If an attacker steals the legitimate access credentials of a partner, the attacker can access your data center disguised as a legitimate user. Then, from the “soft, chewy interior” of your network, the attacker can use your internal servers and endpoints to move laterally through the network and compromise critical systems. Once an outside adversary breaches the network, you rely on network and user segmentation and layered defenses inside the network to protect your data, the same as when an attack originates from the inside.

Developing a best practice security policy helps protect your data center from attacks regardless of origin, in a staged and prioritized manner, securing the most valuable assets first and then phasing in additional protection. A gradual transition from a hope-for-the-best security policy to a best practice security policy helps to ensure the confidentiality of your data, the integrity of your organization, and the availability of the data center in a practical way. The following recommendations for designing and implementing a data center best practice security policy show you how to safely enable applications, users, and content by classifying all traffic, all the time, with minimal disruption to end users.
Data Center Best Practice Methodology

The following best practice methodologies ensure detection and prevention at multiple stages of the attack life cycle.

<table>
<thead>
<tr>
<th>Best Practice Methodology</th>
<th>Why Is This Important?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspect All Traffic to Gain Complete Visibility</td>
<td>Seeing network traffic enables you to identify the presence of attackers. Inspect traffic to see the users, applications, and content that flow into, through, and out of the data center:</td>
</tr>
<tr>
<td>Deploy next-generation firewalls in positions where they can inspect all of the network traffic. Don’t allow traffic to flow into the data center or between network segments without positioning a firewall to examine the traffic.</td>
<td></td>
</tr>
<tr>
<td>Enable SSL decryption on all traffic entering or exiting the data center, unless regulations or compliance rules require you to except categories such as health, finance, government, or military. You must see threats to protect your network against them. Because more than 50 percent of a typical network’s traffic is encrypted and that percentage is rising, if you don’t decrypt traffic, you can’t completely protect your network.</td>
<td></td>
</tr>
<tr>
<td>Use App-ID to identify applications, and create custom applications for proprietary applications, so that the firewall can identify and categorize those applications appropriately and apply the correct security policy rule. This is especially important for older legacy applications that are otherwise categorized as “web-browsing” or “unknown-tcp” instead of being correctly categorized.</td>
<td></td>
</tr>
<tr>
<td>If you have existing Application Override policies that you created solely to define custom session timeouts for a set of ports, convert the existing Application Override policies to application-based policies by configuring service-based session timeouts to maintain the custom timeout for each application and then migrating the rule the an application-based rule. Application Override policies are port-based. When you use Application Override policies to maintain custom session timeouts for a set of ports, you lose application visibility into those flows, so you neither know nor control which applications use the ports. Service-based session timeouts achieve custom timeouts while also maintaining application visibility.</td>
<td></td>
</tr>
<tr>
<td>Enable User-ID on all traffic entering or exiting the data center to map application traffic and associated threats in its content to users and services. You enable User-ID on network segments (zones), so you must segment the network to enable User-ID. Segmenting the network is a best practice for gaining visibility and reducing the attack surface.</td>
<td></td>
</tr>
<tr>
<td>Deploy GlobalProtect in internal mode as a gateway to control access to the data center. GlobalProtect checks user information to verify users, and host information to verify that host security is up-to-date, by comparing the host information to HIP objects and profiles that you define. This ensures that hosts connecting to your network maintain your level of security standards.</td>
<td></td>
</tr>
<tr>
<td>Enable “log at session end” on all security policy rules.</td>
<td></td>
</tr>
<tr>
<td>Visibility into traffic enables the firewall to use its native App-ID, Content-ID, and User-ID technologies to tie the applications, threats, and content to users, regardless of user location or device type, port, encryption, or evasive technique.</td>
<td></td>
</tr>
</tbody>
</table>

Reduce the Attack Surface | The attack surface is all of the points of network interaction, both hardware and software, including applications, content, and users, along with servers, switches, routers, and other
Best Practice Methodology | Why Is This Important?
--- | ---
Physical and virtual equipment. Reducing the attack surface leaves fewer vulnerabilities for attackers to target. The more you reduce the attack surface, the harder it is to breach the network.
- Assess your data center so that you know the applications, content, and users on the network.
- Use positive security enforcement by creating application-based security policy rules that allow only applications with a legitimate business use on the network and rules to block all high-risk applications that have no legitimate use case.
- Use the information from assessing the environment to create a strategy that segments the network into zones based on business requirements, common functionality, and global policy requirements, so that the resources in each zone need the same security level. Inside the data center, segment applications tiers such as databases, web servers, application servers, development servers, and production servers into zones. Segmentation enables you to see traffic between different application tiers because the traffic must traverse a firewall when it flows between zones.
- Granular segmentation enables you to construct security policy rules that focus on the business requirements of each zone and provide the appropriate protection to each segment. Segmentation also helps stop lateral movement of malware into and within the data center because the combination of App-ID, Content-ID (threat prevention), and User-ID enable you to identify the traffic that should be allowed access and deny the rest.
- Deploy GlobalProtect in internal mode as a gateway to control access to the data center.
- To further reduce the attack surface, on security policy rules that allow application traffic, apply File Blocking profiles to block malicious and risky file types. Prevent credential theft breaches by using the firewall’s authentication policy to enable Multi-Factor Authentication, so that even if attackers succeed in stealing credentials, they won’t succeed in accessing the data center network.

Prevent Known Threats | Security profiles attached to security policy allow rules scan traffic for known threats such as viruses, spyware, application-layer vulnerability exploits, malicious files, and more. The firewall applies an action such as allow, alert, drop, block IP, or a connection reset to those threats based on the security profile configuration.
Follow content update best practices and install content updates as soon as possible after downloading them to update the security profiles and apply the latest protections to your data center. Security profiles are fundamental protections that are easy to apply to security policy rules.

External dynamic lists (EDLs) also protect against known threats. EDLs import lists of malicious and risky IP addresses, URLs, or domains into the firewall to prevent known threats. EDLs come from trusted third parties, from predefined EDLs on the firewall, and from custom EDLs that you create. EDLs are updated dynamically on the firewall without requiring a commit.

Preventing known threats is another reason that enabling decryption is important. If you can’t see the threat, it doesn’t matter if you know about it, you may still be victimized because you can’t see it.

Prevent Unknown Threats | How do you detect a threat nobody has seen before? The answer is to forward all unknown files to WildFire for analysis.
<table>
<thead>
<tr>
<th>Best Practice Methodology</th>
<th>Why Is This Important?</th>
</tr>
</thead>
<tbody>
<tr>
<td>WildFire identifies unknown or targeted malware. The first time a firewall detects an unknown file, the firewall forwards the file to its internal destination and also to the WildFire cloud for analysis. WildFire analyzes the file (or a link in an email) and returns a verdict to the firewall in as little as five minutes. WildFire also includes a signature that identifies the file, transforming the unknown file to a known file. If the file contained a threat, the threat is now known. If the file is malicious, the next time the file arrives at the firewall, the firewall blocks it.</td>
<td></td>
</tr>
</tbody>
</table>

You can check verdicts in the WildFire submission logs (Monitor > Logs > WildFire Submissions). Set up WildFire appliance content updates to download and install automatically every minute so that you always have the most recent support. For example, support for Linux and SMB files were first delivered in WildFire appliance content updates.

In addition:

- Manage firewalls centrally with Panorama to consistently enforce policy across physical and virtual environments and for centralized visibility.
- Use positive security enforcement to allow traffic you want on your data center network and deny the rest.
- Create a standardized, scalable design that you can replicate and apply consistently across data centers.
- Get buy-in from executives, IT and data center administrators, users, and other affected parties.

Phase in next-generation security by focusing on the most likely threats to your particular business and network, and then determine the most important assets to protect and protect them first. Ask the following questions to help prioritize the assets to protect first:

1. **What makes our company what it is?** What properties define and differentiate your company, and what assets map to those properties? Assets that relate to your company’s proprietary competitive advantages should be high on the protection priority ladder. For example, a software development company would prioritize its source code, or a pharmaceutical company would prioritize its drug formulas.

2. **What keeps the enterprise in business?** Which systems and applications do you need to support the daily operation of the company? For example, your active directory (AD) service provides employee access to applications and workstations. Compromising your AD service gives an attacker access to all accounts within your enterprise, which gives the attacker full access your network. Other examples include critical IT infrastructure such as management tools and authentication servers, and servers that house the most critical data for business operations.

3. **If I lost this asset, what would happen?** The worse the consequences of losing an asset, the higher the priority to protect that asset. For example, the user experience may differentiate a service company, so protecting that experience is high priority. Proprietary processes and equipment may differentiate a manufacturing company, so protecting the intellectual property and proprietary designs is high priority. Create a priority list to define what to protect first.

Define the ideal future state of your data center network and work in phases to achieve it. Periodically revisit your definition to account for changes in your business, new regulatory and legal requirements, and new security requirements.
How Do I Deploy a Data Center Best Practice Security Policy?

The workflow for implementing a data center best practice security policy is to learn about your data center network, its assets, and the firewall's threat prevention capabilities, and then create initial security policy rules based on that information, protecting your most valuable assets first.

- **How to Assess Your Data Center**—Identify and prioritize the assets to protect, the biggest threats to those assets, and the applications and users sanctioned for access.
- **How to Decrypt Data Center Traffic**—You can't protect your network against threats you can't see. Encrypted traffic is a common method for attackers to deliver threats.
- **Create a Data Center Segmentation Strategy**—Segmenting your data center prevents an adversary who gains a foothold in the data center from moving laterally to other areas.
- **How to Create Data Center Best Practice Security Profiles**—Legitimate applications can deliver command and control malware, common vulnerabilities and exposures (CVEs), drive-by downloads of malicious content, phishing attacks, and APTs. Best practice Security Profiles protect allowed traffic from known and unknown threats for all four data center traffic flows.
- **Use Traps to Protect Data Center Endpoints**—Firewalls protect against threats that traverse the network. But threats that execute on an endpoint don’t cross the network, so they don't traverse a firewall. Install Traps on every endpoint to protect against threats on the endpoints themselves.
- **Create Data Center Traffic Block Rules**—Block known malicious IP addresses, applications that attackers commonly exploit, applications designed to evade or bypass security, and applications that you don’t need for business purposes in the data center.
- **Define the Initial User-to-Data-Center Traffic Security Policy**—Unauthorized access poses a huge risk to the valuable information inside the data center. Because employees and other users on the internal corporate network are often trusted, security precautions may be lax. The user population and the data center may even be on one flat network. Tightly control who can access the data center, the assets different user groups can access, and the level of access different user groups have to applications.
- **Define the Initial Internet-to-Data-Center Traffic Security Policy**—Protect data center servers from malicious internet traffic. Exploiting server-side vulnerabilities opens the data center to attack and puts partners at risk because a compromised data center server could serve exploits to third-party clients.
- **Define the Initial Data-Center-to-Internet Traffic Security Policy**—Command-and-control malware hiding on an infected internet-connected server can use legitimate applications to download more malware. Prevent applications from using non-standard ports, permit transfers of only the file types that each application should legitimately use, and block URL categories for malware, phishing, proxy anonymizer, peer-to-peer, and other potentially malicious URL categories.
- **Define the Initial Intra-Data-Center Traffic Security Policy** (East-West Traffic)—Threats from within the data center are often overlooked because no user traffic originates there and within the data center is considered as trusted. However, if an attacker compromises a data center server, communication between servers and VMs can spread malware. The best practice Security policy prevents attackers from moving laterally through the data center and compromising more systems or exfiltrating data.
- **Log and Monitor Data Center Traffic**—Logging and monitoring allows us to track and maintain your data center best practice security policy. It reveals the applications, users, and traffic patterns on your network, including those you may not have known were there. This information helps you investigate potential security issues.
- **Maintain the Data Center Best Practice Rulebase**—Continually monitor your application whitelist so that you can adapt your rules to accommodate new sanctioned applications and determine how new or modified App-IDs impact your policy.

**Order the Data Center Security Policy Rulebase** summarizes the Security policy rulebase.
How to Assess Your Data Center

To achieve a Zero Trust security model, you need to know and evaluate the assets in your data center so that you can prioritize protecting the most valuable assets first, determine who should have access to those assets, and understand the major risks to those assets. Understanding the users who access the assets, the allowed applications, and the network itself enables you to evaluate what you need and what you trust, so that you can craft a data center best practice security policy that allows only user access and applications that have legitimate business purposes on the network.

1. **Inventory the data center environment**—Inventory the physical and virtual data center environments, including servers, routers, switches, security devices, and other network infrastructure, and inventory the data center applications (including internally developed custom applications) and service accounts.
   - Assess each system based on its role in the network and its importance to the business to prioritize which portions of the physical and virtual infrastructure to protect first. For example, if your business involves credit card transactions, the servers that handle credit card transactions and the path of communication for traffic carrying credit card information are extremely valuable assets whose protection should be prioritized.
   - Examine at least 90 days of traffic logs to inventory the applications on the data center network. Create a custom report based on the data center’s application database to help identify the existing data center applications. Use the data center application inventory to develop a whitelist of applications you want to sanction or tolerate on your data center network, including internally developed custom applications.
     
     **Your initial application inventory doesn’t need to identify every application because by monitoring the block rules that you configure for the data center best practice security rulebase, you’ll discover the applications you haven’t identified. Focus on inventorying the applications and application types that you want to allow. When you finish developing the application whitelist, all applications that you don’t explicitly allow are denied.**

     Map the applications to business requirements. If an application doesn’t map to a business requirement, evaluate whether you should tolerate it on the network. Applications that meet no apparent business need increase the attack surface and may be part of an attacker’s tool set. Even if an unneeded application is innocent, the best practice is to remove it so that there is one less surface for an attacker to exploit. If multiple applications perform the same function, for example, file sharing or instant messaging, consider standardizing on one or two applications to reduce the attack surface.

     If any internal custom applications don’t use the application-default port, note the ports and services required to support the custom application. Consider rewriting internal custom applications to use the application-default port.

     **Create groups for applications** that require similar treatment on the network so that you apply security policy efficiently to application groups rather than to individual applications. Application groups make designing and implementing security policy easier because you can apply policy to all of the applications in a group at one time, change policy for the entire group, add new applications to the group to apply the group’s policy to the new applications, and reuse an application group in multiple security policy rules. For example, an application group designed for data center storage applications may include applications such as crashplan, ms-ds-smb, and NFS.

     - Inventory the service accounts that applications use to communicate between servers and within servers inside the data center. A best practice is to use one service account for each function instead of using one service account for multiple functions. This limits access to the service account and makes it easier to understand how the service account was used if a system is compromised. Another best practice is to identify service accounts that are hard-coded into the application so that you can write IPS signatures against them and monitor the use of the accounts.
2. **Characterize data center traffic**—Characterize and map data center traffic to understand how data flows across your network and between users and resources. Engage a cross-functional team that includes application architects, network architects, enterprise architects, and business representatives. Characterizing the traffic flows informs you about network traffic sources and destinations, typical traffic patterns and loads, and helps you understand the traffic on your network and prioritize the most important traffic to protect. Use Application Command Center widgets, Panorama’s firewall health monitoring features, and other methods to understand the normal (baseline) traffic patterns, which helps you understand abnormal traffic patterns that may indicate an attack.

3. **Assess data center segmentation**—Segment data center server tiers so that communication between different server tiers must pass through the next-generation firewall to be decrypted, examined, and protected by the best practice security policy, and so that communication from the user population or the internet passes through a next-generation firewall. Outside the data center, understand which zones can communicate with each data center zone, and then determine which zones should be allowed to communicate with each data center zone.

4. **Assess user population segmentation and determine who should have access to the data center**—Map users to groups to segment the user population so that you can more easily control access to sensitive systems. For example, users in the Product Management group should not be able to access finance or human resource systems. In Active Directory (or whatever system you use), create granular groups of users based on the access level the users require for legitimate business purposes so that you can control access to systems and applications. This includes different employee groups as well as different contractor, partner, customer, and vendor groups, grouped by the level of access needed.

Reduce the attack surface by creating user groups based on access requirements rather than just functionality, and grant only the appropriate level of application access to each group. Within a functional area such as Marketing or Contractors, create multiple user groups mapped to application access requirements.

5. **Continuously monitor the data center network**—Log and Monitor Data Center Traffic to reveal gaps in the data center best practice security policy, to expose unusual traffic patterns or unexpected access attempts that may indicate an attack, and to diagnose application issues.

A helpful method for evaluating assets is grouping assets. Identify your most valuable assets that need to be protected first, and identify the assets that you can iterate on after protecting those assets. Prioritize the order in which to protect the assets in each category. Organize assets in the way that makes the most sense for your particular business. The following table shows you some possibilities, but it’s not comprehensive. Also consider legal compliance requirements to protect data such as passwords, personal information, and financial information when prioritizing which assets to protect first.

**Table 1: Example Asset Categories**

<table>
<thead>
<tr>
<th>Most Valuable Assets</th>
<th>Other Valuable Assets</th>
<th>Remaining Assets (Iterate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patents</td>
<td>Critical IT infrastructure such as router and firewall interfaces</td>
<td>Network lab equipment</td>
</tr>
<tr>
<td>Source code</td>
<td>Authentication services</td>
<td>IT management systems</td>
</tr>
<tr>
<td>Confidential data such as product designs, drug formulas, or user data.</td>
<td>Email</td>
<td>Other assets</td>
</tr>
<tr>
<td>Proprietary algorithms</td>
<td>VPNs, especially for highly distributed enterprises</td>
<td></td>
</tr>
<tr>
<td>Code signing certificates and PKI (these are the keys to your encrypted kingdom)</td>
<td>Critical business applications</td>
<td></td>
</tr>
<tr>
<td>AD domain server (losing the AD enables an attacker to create credentials that provide unlimited network access)</td>
<td>File sharing servers</td>
<td></td>
</tr>
<tr>
<td>Databases</td>
<td>Databases</td>
<td></td>
</tr>
</tbody>
</table>
Most Valuable Assets | Other Valuable Assets | Remaining Assets (Iterate)
---|---|---
• Other highly prized assets that set your business apart from other businesses

Asset priority is unique to each business. For a service company, the user experience may differentiate the business from other businesses, so the most valuable assets may be assets that ensure the best user experience. For a manufacturing company, the most valuable assets may be proprietary processes and equipment designs. Considering the consequences of losing an asset is a good way to figure out which assets to protect first.
How to Decrypt Data Center Traffic

You can't protect your network against threats you can't see. Decrypting traffic to expose malware is critical because more than 60 percent of a typical network's traffic is encrypted and the percentage is rising. Gartner predicts that through 2019, more than 80 percent of enterprise web traffic will be encrypted, and during 2019, more than 50 percent of new malware campaigns will use various forms of encryption and obfuscation to conceal delivery and ongoing communications, including data exfiltration.

To expose encrypted applications and threats, position physical or virtual next-generation firewalls so they see all data center traffic. The best practice is to decrypt all the traffic you can, especially high-risk traffic categories and traffic destined for critical servers. Decrypting traffic correctly identifies it so that the firewall can apply antivirus, vulnerability protection, WildFire, and other protections appropriately.

To apply decryption to traffic, create decryption profiles that specify how to handle SSL and SSH traffic and traffic that you choose not to or can't decrypt. Decryption profiles enable you to set the allowed algorithms, modes, and session characteristics for traffic. You apply Decryption profiles to Decryption policy rules, which specify the traffic to which the firewall applies the Decryption profiles.

The firewall supports two types of SSL/TLS decryption and SSH decryption:

- SSL forward proxy
- SSL inbound inspection
- SSH proxy

Within the data center, decrypt as much east-west traffic as possible. If performance considerations due to incorrect firewall sizing prevent you from decrypting all traffic, prioritize the most critical servers, the highest risk traffic categories, and less trusted segments and IP subnets, and decrypt as much traffic as you can while retaining acceptable performance. Key questions to ask are: “What happens if this server is compromised?”, “How much risk does each category of traffic represent?”, and “How much risk am I willing to take in relation to the level of performance I want to achieve inside the data center?”

For traffic flowing from the data center to the internet, decrypt everything except traffic for which you must make exceptions. Decryption's visibility is especially important because you don't want servers in the data center to connect to malicious sites, transfer malicious files, or be vulnerable to malware downloads.

When you plan your decryption policy, consider your company's security compliance rules and positions. For traffic from users to the data center, although a tight Decryption policy may initially cause a few complaints, those complaints can draw your attention to unsanctioned or undesirable websites that are blocked because they use weak algorithms or have certificate issues. Use complaints as a tool to better understand the traffic on your network.

Decryption traffic consumes firewall resources. The amount of traffic to decrypt varies with each data center. When sizing the firewall deployment to maintain acceptable performance while supporting decryption, take into account the amount of traffic you expect to decrypt (some applications must be decrypted while other applications aren't encrypted and don't need to be decrypted), the decryption cipher (stronger, more complex ciphers require more processing power to decrypt), the size of the keys (larger keys consume more decryption resources), the type of key exchange (for example, RSA key exchanges consume more processing resources than PFS keys), and the capacity of the firewalls. Work with your Palo Alto Networks sales team and representatives to size the firewall deployment appropriately for your particular network so that you can decrypt traffic and expose threats.

Companies with businesses such as banking that require extremely strong security for their private keys can use a third-party hardware security module (HSM) to safeguard and manage the company's private key instead of storing it on the firewall.

- Create the Data Center Best Practice Decryption Profiles
• Exclude Unsuitable Traffic from Data Center Decryption

Create the Data Center Best Practice Decryption Profiles

Decryption profiles specify how the firewall checks decrypted traffic and also traffic that you either can’t or choose not to decrypt. The firewall checks protocols, server certificates, session characteristics, and ciphers (key exchange algorithms, encryption algorithms, and authentication algorithms). You apply Decryption profiles (Objects > Decryption Profile) to Decryption policy rules (Policies > Decryption). Decryption policy rules define the traffic to check using the source, destination, service category, and URL category as match criteria so that you have granular control over the traffic to which you apply a Decryption profile.

To decrypt outbound traffic, the firewall acts as an SSL forward proxy device between the internal client and the external server. To inspect inbound traffic, the firewall makes a copy of the incoming session traffic and decrypts and inspects the copy.

STEP 1 | Configure the firewall to perform CRL/OCSP checks to ensure that certificates presented during SSL decryption are valid.

STEP 2 | Configure the SSL Decryption > SSL Protocol Settings to block vulnerable SSL/TLS versions such as TLS 1.0 and SSLv3, and to avoid weak encryption algorithms such as RC4 and 3DES, and weak authentication algorithms such as MD5 and SHA1.

SSL Protocol Settings apply to all decrypted traffic.

Set the Min Version to TLSv1.2 to provide the strongest security—business sites that value security support TLSv1.2. If a site (or a category of sites) only supports weaker ciphers, review the site and determine if it really houses a legitimate business application. If it does, make an exception for only that site by configuring a Decryption profile with a Min Version that matches the strongest cipher the site supports and applying it to a Decryption policy rule that limits the weak cipher to only the site or sites in question. If the site doesn’t house a legitimate business application, don’t weaken your security posture to support the site—weak protocols (and ciphers) contain known vulnerabilities that attackers can exploit. If the site belongs to a category of sites that you don’t need for business purposes, use URL Filtering to block access to the entire category. Don’t support weak encryption or authentication algorithms unless you must do so to support important legacy sites.
Set the Max Version to Max rather than to a particular version so that as the protocols improve, the firewall automatically supports the newest and best protocols. Whether you intend to attach a Decryption profile to a Decryption policy rule that governs inbound (SSL Inbound Inspection) or outbound (SSL Forward Proxy) traffic, avoid allowing weak algorithms.

**STEP 3** | Configure the SSL Decryption > SSL Forward Proxy settings for outbound traffic to block exceptions during SSL negotiation and block sessions that can't be decrypted.

In some cases, the best practice settings depend on your company’s security compliance rules. Apply the SSL Forward Proxy Decryption profile to security policy rules that control outbound traffic.

Block exceptions during SSL negotiation and block sessions that can’t be decrypted.

- **Server Certificate Verification**—Whether to check the **Block sessions on certificate status check timeout** box depends on your company’s security compliance stance because it’s a tradeoff between tighter security and a better user experience. Certificate status verification examines the Certificate Revocation List (CRL) on a revocation server or uses Online Certificate Status Protocol (OCSP) to find out if the issuing CA has revoked the certificate and the certificate should not be trusted. However, revocation servers can be slow to respond, which can cause the session to timeout and the firewall to block the session even though the certificate may be valid. If you **Block sessions on certificate status check timeout** and the revocation server is slow to respond, you can use **Device > Setup > Session > Decryption Settings** and click **Certificate Revocation Checking** to change the default timeout value of five seconds to another value.
Enable both CRL and OCSP certificate revocation checking because server certificates can contain the CRL URL in the CRL Distribution Point (CDP) extension or the OCSP URL in the Authority Information Access (AIA) certificate extension.

Although the best practice is to use a proper certificate, some certificates leave the Subject Alternate Name (SAN) field blank, which can cause firewalls to reject those certificates. Check **Append certificate’s CN value to SAN extension** to automatically copy the certificate number to the SAN field if the SAN field is blank, so that if you do business with sites that don’t populate the certificate’s SAN field, you can accept their certificates. Otherwise, the sites need to regenerate their certificates to conform to proper practice and populate the SAN field.

Block all other server certificate verification exceptions.

- **Unsupported Mode Checks**—If you don’t block sessions with unsupported versions and unsupported cipher suites, then users receive a warning message that they can click through to reach the risky website. The reason you configure tight SSL Protocol Settings is to block and protect you from servers that use these weak (risky) protocol versions and algorithms. In addition, blocking sessions with unsupported mode checks protects you from malicious backdoors and other threats that use custom and non-standard encryption to obfuscate their activities.

**Block sessions with client authentication** enables you to choose whether to allow or block sessions that use client authentication. Although server authentication can be the only authentication used to establish a session, some sites use mutual authentication, where both the server and the client authenticate to establish a session. Client authentication using an X.509 Digital Certificate is similar to server authentication in that both methods use a digital certificate issued by a trusted Certificate Authority to authenticate a session. The client certificate acts as a digital identifier for the client, resides on the client device, and can’t be ported to other devices. However, client authentication prevents the firewall from decrypting the session because the firewall needs both the client and server certificates to perform bi-directional decryption, but the firewall only knows the server certificate. This breaks decryption for client authentication sessions.

If you don’t check **Block sessions with client authentication**, when the firewall attempts to decrypt a session that uses client authentication, the firewall allows the session and adds an entry in its local decrypt exclude cache that contains the server URL/IP address, the application, and the Decryption profile. Entries remain in the cache for 12 hours and then age out. If the same user or a different user attempts to access the server within 12 hours using client authentication, the firewall matches the session to the decrypt exclude cache entry, does not attempt to decrypt the traffic, and allows the encrypted session.

If the exclude cache becomes full, the firewall purges the oldest entries as new entries arrive. If you change the Decryption policy or profile, the firewall flushes the exclude cache because changing the policy or profile can change the classification outcome of the session.

If you check **Block sessions with client authentication**, the firewall blocks sessions that use client authentication, with the exception of sessions from sites on the SSL Decryption Exclusion list (Device > Certificate Management > SSL Decryption Exclusion).

You may need to allow traffic on your network from other sites that use client authentication in addition to the Predefined sites on the SSL Decryption Exclusion list. Create a Decryption profile that allows sessions with client authentication. Add it to a Decryption policy rule that applies only to the server(s) that house the application. To increase security even more, you can require Multi-Factor Authentication to complete the user login process.

For all other traffic, apply the Decryption profile that blocks sessions with client authentication.

- **Failure Checks**—If you don’t **Block sessions if resources not available**, the risk is that a lack of processing resources may allow potentially dangerous connections. If you block sessions for which resources aren’t available, it may affect the user experience. Whether to implement failure checks depends on your company’s security compliance stance and the importance to your business of the user experience, weighed against tighter security.
If you use a Hardware Security Module (HSM) to store your private keys, whether you check **Block sessions if HSM not available** depends on your compliance rules about where the private key must come from and how you want to handle encrypted traffic if the HSM isn’t available. For example, if your company mandates the use of an HSM for private key signing, then block sessions if the HSM isn’t available. However, if your company is less strict about this, then you can consider not blocking sessions if the HSM isn’t available. (If the HSM is down, the firewall can process decryption for sites for which it has cached the response from the HSM, but not for other sites.) The best practice in this case depends on your company’s policies. If the HSM is critical to your business, run the HSM in a high-availability (HA) pair (PAN-OS 8.0 supports two members in an HSM HA pair).

**STEP 4** | Configure the **SSL Decryption > SSL Inbound Inspection** settings to inspect traffic from an external client to your internal servers and block suspicious sessions.

Apply the SSL Inbound Inspection Decryption profile to security policy rules that control inbound traffic.

- **Unsupported Mode Checks**—The firewall can’t decrypt session versions and ciphers that the firewall doesn’t support. To prevent attackers from using unsupported versions and ciphers to sneak onto the network, block session versions and cipher suites that the firewall doesn’t support. In addition, blocking sessions with unsupported mode checks protects you from malicious backdoors and other threats that use custom and non-standard encryption to obscure their activities.

On the server, enable only the ciphers that you support on the firewall. Ensuring this compatibility makes the negotiation between the client and the server smoother.

- **Failure Checks**—If you don’t **Block sessions if resources not available**, the risk is that a lack of processing resources may allow potentially dangerous connections. If you block sessions for which resources aren’t available, it may affect the user experience. Whether to implement failure checks depends on your company’s security compliance stance and the importance to your business of the user experience, weighed against tighter security.

If you use a Hardware Security Module (HSM) to store your private keys, whether you check **Block sessions if HSM not available** depends on your compliance rules about where the private key must come from and how you want to handle encrypted traffic if the HSM isn’t available. For example, if your company mandates the use of an HSM for private key signing, then block sessions if the HSM isn’t available. However, if your company is less strict about this, then you can consider not blocking sessions if the HSM isn’t available. (If the HSM is down, the firewall can process decryption for sites for which it has cached the response from the HSM, but not for other sites.) The best practice in this case depends on your company’s policies. If the HSM is critical to your business, run the HSM in a high-availability (HA) pair (PAN-OS 8.0 supports two members in an HSM HA pair).

**STEP 5** | For SSH traffic, configure **SSH Proxy** Decryption profile settings.
SSH Decryption allows normally routed SSH traffic and denies SSH tunneling (SSH port forwarding) traffic, but doesn’t perform content or threat inspection on the SSH traffic. SSH tunneling sessions can tunnel X11 Windows packets and TCP packets. One SSH connection may contain multiple channels. When you apply an SSH Decryption profile to traffic, for each channel in the connection, the firewall examines the App-ID of the traffic and identifies the channel type. The channel type can be:

- session
- X11
- forwarded-tcpip
- direct-tcpip

When the channel type is session, the firewall identifies the traffic as allowed SSH traffic such as SFTP or SCP. When the channel type is X11, forwarded-tcpip, or direct-tcpip, the firewall identifies the traffic as SSH tunneling traffic and blocks it.

For most user groups, you probably won’t allow SSH traffic in the data center. SSH is usually used for remote access to servers, which is not a capability you want most users to have because it places your data center servers at greater risk, for access to Linux servers, and for file transfers. You can’t decrypt SSH traffic, so anyone who uses SSH to access data center resources must be trusted—and even so, all of the threat profiles should be attached to any rule that allows SSH access to scan for malware, viruses, spyware, etc.

An example use case for SSH is IT personnel who manage and maintain data center servers and use SSH for remote access.

**Unsupported Mode Checks**—The firewall can’t decrypt session versions and ciphers that the firewall doesn’t support and unsupported versions and ciphers may be vulnerable. To prevent attackers from using unsupported versions and ciphers to sneak onto the network, block session versions and cipher suites that the firewall doesn’t support. In addition, blocking sessions with unsupported mode checks protects you from malicious backdoors and other threats that use custom and non-standard encryption to obscure their activities.

**Failure Checks**—If you don’t Block sessions if resources not available, the risk is that a lack of processing resources may allow potentially dangerous connections. If you block sessions for which resources aren’t available, it may affect the user experience. Whether to implement failure checks depends on your company’s security compliance stance and the importance to your business of the user experience, weighed against tighter security.

**STEP 6** | For traffic that you choose not to decrypt, configure the No Decryption settings to block encrypted sessions destined for sites with expired certificates or untrusted issuers.
Apply the No Decryption profile only to traffic that you choose not to decrypt because of regulations or compliance rules, not to traffic that can’t be decrypted because of technical reasons, such as a pinned certificate. The best practice is to decrypt as much data center traffic as possible.

Exclude Unsuitable Traffic from Data Center Decryption

Two types of traffic are unsuitable for decryption:

- Traffic that breaks decryption because of technical reasons such as using client certificate authentication, a pinned certificate, or an incomplete certificate chain.
- Traffic that you choose not to decrypt.

The firewall provides a predefined SSL Decryption Exclusion list (Device > Certificate Management > SSL Decryption Exclusion) for commonly used sites that break decryption because of technical reasons. You can remove predefined sites from the list by clicking the checkbox next to the site hostname and then clicking Disable, and you can add sites to the list. Use the Decryption Exclusion list only for sites that break decryption for technical reasons, don’t use it for sites that you choose not to decrypt. If decryption breaks an important application, add it to the Decryption Exclusion list to create an exception for the specific IP address, domain, or common name in the certificate associated with the application. Some internal custom applications may break if you decrypt them.

If the technical reason for excluding a site from decryption is an incomplete certificate chain, the next-generation firewall doesn’t automatically fix the chain like a browser. If you need to add a site to the SSL Decryption Exclusion list, manually review the site to ensure it’s a legitimate business site, then download the missing sub-CA certificates and load and deploy them onto the firewall.

You may choose not to decrypt traffic for reasons such as regulations and legal compliance. For example, the European Union (EU) General Data Protection Regulation (GDPR) will require strong protection of all personal data for all individuals. The GDPR affects all companies, including foreign companies, that collect or process the personal data of EU residents. Different regulations and compliance rules may mean that you treat the same data differently in different countries or regions. Businesses usually can decrypt personal information in their corporate data centers because the business owns the information. The best practice is to decrypt as much traffic as possible so that you can see it and apply security protection to it.

For traffic you choose not to decrypt, make sure it really is traffic you don’t want to decrypt, and then create a policy-based exclusion that specifies the application, user group, source and destination, URL category, and/or service to limit each exclusion as much as possible. The more specific the decryption exclusion, the better, so that you don’t inadvertently exclude more traffic than necessary from decryption.
Create a Data Center Segmentation Strategy

A flat, unsegmented network is difficult to defend because if an attacker gains access to the network, the attacker can move laterally and compromise critical systems. This is especially true inside the data center, where companies keep their most valuable assets. Old segmentation methods such as VLANs don't scale well, are difficult to automate, and don't take into account users, content, or applications, so they provide little control over or visibility into traffic.

Create a segmentation strategy that provides more granular access control to data center resources, which gives you better visibility into traffic. The more granular your segmentation strategy, the more visibility into traffic you gain because traffic must traverse a firewall (segmentation gateway) as it flows between segments. Segmentation also makes compliance and compliance audits easier because you can prevent all but the necessary access to personal information, which protects the data and reduces the scope of audits.

Your data center segmentation strategy depends on your architecture and your business goals, so there is no “one size fits all” implementation. However, learning common guidelines enables you to design and implement a segmentation strategy to protect your data center network.

- How to Segment the Data Center
- How to Segment Data Center Applications

How to Segment the Data Center

How you segment your data center depends on your business requirements and your data center network architecture, including your SDN solution, which may dictate the segmentation method. For example, vwire interfaces control firewall connectivity on an NSX host. Because vwire interfaces don't route or switch traffic on an NSX host, they must belong to the same zone, so all of the resources for a particular tenant (department, customer, or application tier) reside in one zone and the firewall uses dynamic address groups to segment application traffic within that zone. Each tenant has a separate zone with its own vwire interfaces. For other SDN solutions, separate virtual firewall instances may segment traffic.

Next generation Palo Alto Networks firewalls provide flexible tools to segment traffic:

- **Zones**—Traffic that crosses zones goes through the firewall for inspection. All allowed data center communication should traverse a firewall and undergo full threat inspection (antivirus, anti-spyware, vulnerability protection, file blocking, WildFire analysis, and URL Filtering for data center traffic that leaves the enterprise and for applications hosted by customer tenants). By default, the firewall denies all traffic between zones (intrazone traffic). You must write specific security policy rules to allow traffic to pass between zones, so only traffic that you explicitly allow can move from one zone to another. How you use zones to segment your data center depends on what assets you need to separate from other assets. For example, a common architecture includes separate zones for development servers and production servers. You can use zones to segment servers that house extremely sensitive information such Payment Card Information (PCI) or Personally Identifiable Information (PII), to segment different internal company departments such as Marketing, Engineering, and Human Resources, and to segment customer resources and customer-hosted applications.

Consider using zone protection profiles to protect zones against floods, reconnaissance activities (port scans and host sweeps), Layer 3 packet-based attacks, and non-IP protocol (Layer 2) packet-based attacks.

- **Dynamic address groups**—For this purpose, dynamic address groups are lists of IP addresses that the firewall imports and uses in security policy to define server groups dynamically instead of statically. Adding and removing IP addresses from a dynamic address group updates security policy automatically, without a commit action on the firewall. Within a zone, using dynamic address groups in security policy whitelist rules allows server-to-server interaction for specified applications and services. For example, in NSX, use dynamic address groups to segment the server tiers within an application tier.
• **User-ID**—Enable User-ID to create application whitelist rules based on user groups to segment users from applications and server groups.

When you design your data center segmentation plan, keep in mind the following general guidelines:

• **How to Assess Your Data Center**, so that you can segment it in stages and protect the most valuable and sensitive assets first.

• Use an SDN solution (such as NSX, ACI, OpenStack) inside the data center to provide a scalable, agile, virtualized infrastructure. SDN is the best way to centralize data center network management, maximize compute resource utilization, scale and automate the network, and control and secure traffic on a virtualized network. Although you can create a non-SDN architecture that essentially replicates an SDN architecture, it’s difficult and time consuming to do, prone to errors that result in outages, and is not considered a best practice. SDN solutions maximize the use of the underlying data center compute resources without sacrificing security.

• Use physical next-generation firewalls to segment and secure non-virtualized legacy servers and use VM-Series firewalls to segment and secure the virtual data center network.

• Group assets that perform similar functions and require the same level of security in the same data center segment. For example, place servers that connect to the internet in the same segment.

Base your segmentation plan on multiple criteria to develop the right plan to secure your business.

### How to Segment Data Center Applications

Segment data center applications to prevent malware from moving between applications and to safely enable those applications for users. **Application tiers** provide the resources and functions required for data center applications. An application tier consists of multiple **server tiers** that work together to fulfill requests and commands related to a particular application. Typically, an application tier consists of three server tiers:

• **Web server tier**—Application interface to users.

• **Application server tier**—Takes requests from the web server tier to process and generate application functionality.

• **Database server tier**—Contains data the application requires to function.

Each server tier contains functionally similar servers that work together so that an application tier can present an application to a user.

### Typical Application Tier

The server tiers within each application tier create a *service chain* of VMs. Service chains steer traffic through virtual data center appliances to provide application services. Within an application tier, a web server may communicate with an application server that houses the application code, and that application server may communicate with a database server that houses content. The communication between the three servers, which reside in different server tiers within an application tier, is the service chain.

Data centers contain many application tiers, which may be dedicated to particular departments, customers, contractors, or other groups. Segment the data center application infrastructure to prevent unauthorized and unnecessary communication among application resources and to inspect application traffic.
<table>
<thead>
<tr>
<th>Application Segmentation</th>
<th>How to Segment Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application tier</td>
<td>Segment the server tiers within each application tier by configuring a separate firewall zone for each server tier, so that you can control access to each set of servers and examine the traffic flowing between each server tier as it traverses the firewall. For example, place web servers, application servers, and database servers in separate zones so that traffic between server tiers always goes through a next-generation firewall for full inspection. Depending on business requirements, you may need to create more than one zone for each application tier to separate tenants, to load balance, to use application tiers for different purposes, to provide different levels of security, or to connect to different sets of servers. Segment the data center to reduce the attack surface of each application tier by grouping in the same zone only servers that require similar levels of trust and that need to communicate with similar application tiers.</td>
</tr>
<tr>
<td>Web server tier</td>
<td>Traffic normally enters the data center through web servers, although there are special cases such as IT configuring direct secured access to data center servers for management purposes. As with the other server tiers, create a separate zone for the web server tier so that you can apply granular security policy to it. Because the web server tier communicates with devices that reside outside the data center, it’s an appealing target for attackers. Place the web server tier on a separate network, for example, using a VLAN. All traffic in and out of the VLAN—all traffic that enters or exits the data center—should traverse a next-generation firewall. You can do this by configuring the next-generation firewall as the default gateway or by using an SDN solution such as NSX to steer traffic. Segment servers within the web server tier to prevent them from communicating with each other, for example, by using a traditional rule such as NSX Distributed Firewall (DFW) to open a port or block traffic within the tier.</td>
</tr>
<tr>
<td>Infrastructure service application servers</td>
<td>Segment the servers that provide critical infrastructure services such as DNS, DHCP, and NTP, and allow access only to their specific IP addresses, using only the appropriate applications.</td>
</tr>
<tr>
<td>Applications</td>
<td>Use App-ID to create application-based whitelist security policy rules that segment applications by controlling who can access each application and on which sets of servers (using dynamic address groups). App-ID enables you to apply granular security policy rules to applications that may reside on the same compute resource but require different levels of security and access control. Create custom applications to uniquely identify proprietary applications and segment access. If you have existing Application Override policies that you created solely to define custom session timeouts for a set a of ports, convert the existing Application Override policies to application-based policies by configuring service-based session timeouts to maintain the custom timeout for each application and then migrating the rule the an application-based rule. Application Override policies are port-based. When you use Application Override policies to maintain custom session timeouts for a set of ports, you lose application visibility into those flows, so you neither know nor control which applications use the ports. Service-based session timeouts achieve custom timeouts while also maintaining application visibility.</td>
</tr>
<tr>
<td>Application Segmentation</td>
<td>How to Segment Applications</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>For migrating from a port-based security policy with custom application timeouts to an application-based policy, don't use Application Override rules to maintain the custom timeouts because you lose visibility into the applications. Instead, define a service-based session timeout to maintain the custom timeout for each application, and then migrate the rule to an application-based rule.</td>
</tr>
</tbody>
</table>

Don't use next-generation firewalls to segment servers within a particular server tier. When you need to prevent intercommunication of servers within a server tier, use a traditional rule such as NSX DFW to open a port or block traffic within the tier. However, servers within a server tier often need to intercommunicate. For example, a database server tier may be a server cluster that requires free intercommunication.
How to Create Data Center Best Practice Security Profiles

Security profiles provide fundamental protections by scanning traffic that you allow on the network for threats. Security profiles provide a full suite of coordinated threat prevention tools that block peer-to-peer command and control (C2) application traffic, dangerous file types, attempts to exploit vulnerabilities, and antivirus signatures, and also identify new and unknown malware.

It takes relatively little effort to apply security profiles because Palo Alto Networks provides predefined profiles that you can simply add to security policy allow rules. Customizing security profiles is easy because you can clone a predefined profile and then edit it. Of course, you can also create a security profile from scratch on the firewall or on Panorama.

To detect known and unknown threats in your network traffic, attach security profiles to all security policy rules that allow traffic on the network, so that the firewall inspects all allowed traffic. The firewall applies security profiles to traffic that matches the security policy allow rule, scans traffic in accordance with the security profile settings, and then takes appropriate actions to protect the network. The recommendations for best practice security profiles apply to all four of the data center traffic flows except as noted.

Download content updates automatically and install them as soon as possible so that you have the latest threat prevention signatures and content (antivirus, anti-spyware, vulnerabilities, malware, etc.) on the firewall and block the latest threats.

- Create the Data Center Best Practice Antivirus Profile
- Create the Data Center Best Practice Anti-Spyware Profile
- Create the Data Center Best Practice Vulnerability Protection Profile
- Create the Data Center Best Practice File Blocking Profile
- Create the Data Center Best Practice WildFire Analysis Profile

You don’t need a URL Filtering subscription for data center firewalls if there is no direct outbound connection to the internet. Firewalls that don’t connect directly to the internet don’t need the PAN-DB URL Filtering solution because it identifies internet URLs, not private data center URLs, so importing the PAN-DB database and checking URLs against it doesn’t apply to data center traffic. If you’re not sure whether a firewall has URL traffic, get a trial URL Filtering subscription and set the profile to alert on all URL categories to identify any URL traffic. Otherwise, URL Filtering should take place on firewalls at the network perimeter where user traffic enters and exits the network, not at the data center perimeter. Consider creating custom URL categories (Objects > Custom Objects > URL Category) to identify and control access to internal data center web services.

Create the Data Center Best Practice Antivirus Profile

Clone the default Antivirus profile and edit it. To ensure availability for business-critical applications, take safe transition steps as you move from your current state to the best practice profile. To achieve the best practice profile, modify the default profile as shown here and attach it to all security policy rules that allow traffic. The Antivirus profile has decoders that detect and prevent viruses and malware from being transferred over six protocols: HTTP, SMTP, IMAP, POP3, FTP, and SMB. You can set WildFire actions for all six protocols because the Antivirus profile also enforces actions based on WildFire signatures.

Configure the cloned best practice Antivirus profile to reset both the client and the server for all six protocol decoders and WildFire actions, and then attach the profile to the allow rules for all four data center traffic flows.
Red triangles in the upper right corner of a cell indicates that the action is modified (changed from the default) and the name of the modified profile is **Strict_AV**.

The reason to attach the best practice Antivirus profile to all security policy rules that allow traffic is to block known malicious files (malware, ransomware bots, and viruses) as they attempt to enter the network. For example:

- **Intra data center traffic**—The Antivirus profile, along with the Vulnerability Protection profile, helps prevent attackers from using exploits to leverage vulnerabilities and spread malware and hacking tools laterally between servers inside the data center network.
- **Traffic from the data center to the internet**—The Antivirus profile, along with the Anti-Spyware profile, helps identify and block command and control traffic and initial downloads of malware and hacking tools.

Create the Data Center Best Practice Anti-Spyware Profile

Attach an Anti-Spyware profile to all security policy rules that allow data center traffic. The Anti-Spyware profile detects command-and-control (C2) traffic initiated from spyware installed on a server or endpoint, including categories such as adware, backdoor, browser-hijack, data theft, and keylogging, and prevents compromised systems from establishing an outbound connection from your network.

Clone the predefined strict Anti-Spyware profile and edit it. To ensure availability for business-critical applications, take safe transition steps as you move from your current state to the best practice profile. If you have a sinkhole set up to which you can send traffic for analysis, enable DNS sinkhole with packet capture to help you track down the endpoint that attempted to resolve the malicious domain. The best practice Anti-Spyware profile retains the default **Action** to reset the connection when the firewall detects a medium, high, or critical severity threat, and enables single **packet capture** (PCAP) for those threats.
Don’t enable PCAP for informational activity because it generates a relatively high volume of that traffic and it’s not particularly useful compared to potential threats. Apply extended PCAP (as opposed to single PCAP) to high-value traffic to which you apply the alert Action. Apply PCAP using the same logic you use to decide what traffic to log—take PCAPs of the traffic you log. Apply single PCAP to traffic you block. The default number of packets that extended PCAP records and sends to the management plane is five packets, which is the recommended value. In most cases, capturing five packets provides enough information to analyze the threat. If too much PCAP traffic is sent to the management plane, then capturing more than five packets may result in dropping PCAPs.

The best practice Action on DNS Queries is to block or to sinkhole DNS queries for known malicious domains and when you don’t have visibility into DNS queries, and to enable PCAPs.

Enabling DNS sinkhole identifies potentially compromised hosts that attempt to access suspicious domains by tracking the hosts and preventing them from accessing those domains. Enable DNS sinkhole when the firewall can’t see the originator of the DNS query (typically when the firewall is north of the local DNS server) so that you can identify infected hosts. Don’t enable DNS sinkhole when the firewall can see the...
originator of the DNS query (typically when the firewall is south of the local DNS server; in this case, the firewall's blocking rules and logs provide visibility into the traffic) or on traffic you block.

In addition to protecting hosts with DNS sinkholing, attach the best practice Anti-Spyware profile to all security policy rules that allow traffic to identify infected hosts as traffic leaves the network and to stop attackers by preventing compromised systems from communicating with the malicious C2 network. If a system can’t communicate with the C2 network, the C2 network can’t control the system. For example:

- Traffic from users to the data center, intra data center traffic, and traffic from the internet to the data center—The Anti-Spyware profile blocks peer-to-peer C2 traffic.
- Traffic from the data center to the internet—The Anti-Spyware profile, along with the Antivirus profile, helps identify and block C2 traffic and initial downloads of malware and hacking tools.

### Create the Data Center Best Practice Vulnerability Protection Profile

Attach a **Vulnerability Protection profile** to all security policy rules that allow traffic. The Vulnerability Protection profile protects against buffer overflows, illegal code execution, and other attempts to exploit client- and server-side vulnerabilities to breach and move laterally through the data center network.

Clone the predefined strict Vulnerability Protection profile. To ensure availability for business-critical applications, take **safe transition steps** as you move from your current state to the best practice profile. For the best practice profile, for each rule except `simple-client-informational` and `simple-server-informational`, double-click the **Rule Name** and change **Packet Capture** from `disable` to `single-packet` to enable packet capture (PCAP) for each rule so you can track down the source of potential attacks. Don’t change the rest of the settings. Download **content updates** automatically and install them as soon as possible so that the signature set is always up-to-date.

Don’t enable PCAP for informational activity because it generates a relatively high volume of that traffic and it’s not particularly useful compared to potential threats. Apply extended PCAP (as opposed to single PCAP) to high-value traffic to which you apply the **alert** Action. Apply PCAP using the same logic you use to decide what traffic to log—take PCAPs of the traffic you log. Apply single PCAP to traffic you block. The default number of packets that extended PCAP records and sends to the management plane is five packets, which is the recommended value. In most cases, capturing five packets provides enough information to analyze the threat. If too much PCAP traffic is sent to the management plane, then capturing more than five packets may result in dropping PCAPs.
The reason to attach the best practice Vulnerability Protection profile to all security policy rules that allow traffic is because if you don’t have strict vulnerability protection, attackers can leverage client- and server-side vulnerabilities to compromise the data center. For example:

- Intra data center traffic—A strict Vulnerability Protection profile, along with the Antivirus profile, helps prevent attackers from using exploits to leverage vulnerabilities and spread malware and hacking tools laterally between servers inside the data center network.
- Traffic from the data center to the internet—Vulnerability protection helps prevent infected data center servers from compromising internet servers.
- Traffic from the internet to the data center—A strict Vulnerability Protection profile blocks attempts to compromise data center servers with server-side vulnerabilities. If a server is compromised, vulnerability protection helps prevent the infected server from serving exploits to clients, isolating the infection and protecting your partners and customers from watering hole attacks. Vulnerability protection also stops brute force attacks using the Block IP action. When brute force attack signatures trigger the action, the firewall blocks the attacker’s IP address for a configured period of time. If the brute force attack resumes after the time period expires, the signatures again trigger the blocking action. The brute force attack may continue, but it never succeeds.

Create the Data Center Best Practice File Blocking Profile

Use the predefined strict File Blocking profile to block files that are commonly included in malware attack campaigns and that have no real use case for upload/download. Blocking these files reduces the attack surface. The predefined strict profile blocks batch files, DLLs, Java class files, help files, Windows shortcuts (.lnk), BitTorrent files, .rar files, .tar files, encrypted-rar and encrypted-zip files, multi-level encoded files (files encoded or compressed up to four times), .hta files, and Windows Portable Executable (PE) files, which include .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon, and .pif files. The predefined strict profile alerts on all other file types for visibility into other file transfers so that you can determine if you need to make policy changes.

In some cases, the need to support critical applications may prevent you from blocking all of the strict profile’s file types. Follow the safe transition advice to help determine whether you need to make exceptions in different areas of the network. Review the data filtering logs (Monitor > Logs > Data Filtering) to identify file types used in the data center and talk with business stakeholders about the file types their applications require. Based on this information, if necessary, clone the strict profile and modify it as needed to allow only the other file type(s) that you need to support the critical applications. You can also use the Direction setting to restrict files types from flowing in both directions or block files in one direction but not in the other direction.
The reason to attach the best practice File Blocking profile to all security policy rules that allow traffic is to help prevent attackers from delivering malicious files to the data center through file sharing applications and exploit kits, or by infecting users who access the data center, or on USB sticks.

- Traffic from users to the data center—Attach the strict File Blocking profile to security policy rules for applications that don't entail file sharing or collaboration to block dangerous file types that can deliver exploits and malware.
- Intra data center traffic—Attach the strict File Blocking profile to security policy rules to prevent a compromised server from sharing a malicious file with other servers in the data center. This isolates the infection and prevents the spread of malware through the data center.
- Traffic from the data center to the internet—Limit file transfers to the file types required by the application in use.

If you don't block all Windows PE files, send all unknown files to WildFire for analysis. For user accounts, set the Action to continue to help prevent drive-by downloads where malicious web sites, emails, or pop-ups cause users to inadvertently download malicious files. Educate users that a continue prompt for a file transfer they didn't knowingly initiate may mean they are subject to a malicious download.

Create the Data Center Best Practice WildFire Analysis Profile

The other security profiles detect and block known threats. WildFire protects the data center from unknown threats. Configure the firewall to forward all unknown files to WildFire for analysis using the predefined default profile. Unknown threats can hide in many different file types and successful attacks may not be detected until long after they have done damage. For example, WildFire can identify malware loaded onto a staging server before the attacker can do damage and find vulnerability scanners and lateral movement assistance tools before attackers achieve their goals. WildFire could have prevented a number of large-scale enterprise breaches over the past several years. Any security policy rule that controls traffic that has, will have, or could have file transfer activity should include an enabled WildFire Analysis profile.

Set up WildFire appliance content updates to download and install automatically every minute so that you always have the most recent support. For example, support for Linux files and SMB files were first delivered in WildFire appliance content updates.
The reason to attach the default WildFire Analysis profile to all security policy rules that allow traffic is because WildFire provides the best defense against unknown threats and advanced persistent threats (APTs). For example:

- Traffic from users to the data center—WildFire identifies unknown malware hosted in the data center such as Confluence or SharePoint.
- Intra data center traffic—WildFire identifies unknown malware spreading among the data center servers, which can prevent the exfiltration of data by discovering the malware before it can do damage.
- Traffic from the data center to the internet—Because this traffic downloads executables for software and operating system updates, it's critical to run WildFire on all applications to identify malicious behaviors.

Set up alerts for malware through email, SNMP, or a syslog server so that the firewall immediately notifies you when it encounters a potential issue. The faster you isolate a compromised host, the lower the chance that the previously unknown malware has spread to other data center devices, and the easier it is to remediate the issue.

If necessary, you can restrict the applications and file types sent for analysis based on the traffic's direction.

*WildFire Action settings in the Antivirus profile may impact traffic if the traffic generates a WildFire signature that results in a reset or a drop action. You can exclude internal traffic such as software distribution applications through which you deploy custom-built programs to transition safely to best practices, because WildFire may identify custom-built programs as malicious and generate a signature for them. Check Monitor > Logs > WildFire Submissions to see if any internal custom-built programs trigger WildFire signatures.*
Use Traps to Protect Data Center Endpoints

Traps protects data center endpoints such as servers and VMs against malware and exploits on the endpoint itself, while the next-generation firewall protects against threats that cross the network (and therefore must traverse the firewall) to reach the endpoint. When malware or exploits are already on an endpoint or get onto an endpoint, if the endpoint executes the threat (for example, through an .exe or .dll file), the firewall doesn't see the threat because the action is on the endpoint and no traffic crosses the firewall, so there's nothing for the firewall to see. However, on each endpoint, Traps sees threats in executables, macros in documents, dynamic-link library files, and more. When these threats attempt to run, Traps goes into action on the endpoint itself and protects the endpoint.

Traps and the next-generation firewall provide a double layer of protection to data center endpoints so that the firewall protects endpoints from threats on the network while Traps monitors and protects endpoints against threats that reside on the endpoint. The security policy you configure for endpoints on an Endpoint Security Manager (ESM) and the security policy you configure on Panorama or on the firewall don't conflict because they govern different events at different locations. Traps controls security within each individual endpoint. The firewall controls security of traffic that traverses the firewall.

Install Traps on every data center endpoint. The best practices for Traps in the data center are the same as the best practices for Traps on any endpoint because the context for Traps is always the endpoint itself, so the context “in the data center” or “in a user group” doesn’t matter—Traps protects all endpoints the same way. So the recommended traps deployment process, the malware protection policy best practices, etc., are the same for the data center as for any other area of the network.
Create Data Center Traffic Block Rules

Before you create the application whitelist rules for the four data center traffic flows, create blocking and logging rules to block applications you don’t use in the data center, block known bad applications, and discover applications that you may not know are on your network. Logging blocked traffic provides information about potential attacks to help you investigate them.

When you discover unknown applications, decide whether they should be allowed or whether they represent potential threats. If these rules discover applications that should be allowed, tune the application whitelist rules accordingly. If these rules discover applications that are not legitimate, they may represent potential threats and you can investigate them using the log information. Don’t apply Security Profiles to block rules because the traffic they control never gets into your network.

**If you discover unknown applications that are internal proprietary applications or other types of legitimate applications, create a custom application for each unknown application so that you can identify it and apply security policy to it.**

Order the Data Center Security Policy Rulebase shows you how to order these rules with all of the other rules we create for the four data center traffic flows so that no rule shadows another rule.

**To apply consistent security policy across multiple data centers, you can reuse templates and template stacks so that the same policies apply to every data center. The templates use variables to apply device-specific values such as IP addresses, FQDNs, etc., while maintaining a global security policy and reducing the number of templates and template stacks you need to manage.**

**STEP 1 | Block all applications from user zones on the application-default port to identify unexpected applications.**

This rule discovers applications that users are attempting to use and that you didn’t know were running on your data center. Monitor traffic that matches this rule to determine if it’s a potential threat or if you need to modify your whitelist rules to allow the application. Be sure to place this rule after whitelist rules that allow traffic or this rule will block traffic that you intend to allow.

The following rule is similar to this rule, except that it applies to traffic from any source, not just traffic from user zones. The reason for creating separate rules is that violations of the user-zone rule may indicate that you’re blocking a legitimate application which some users need to conduct business, so you may need to modify a whitelist rule to allow the application for a particular set of users. Violations from non-user zones may indicate a change in an application or a potential attack. Creating a separate rule for the rest of the traffic enables you to view separate logs for user traffic and for all other traffic attempting to enter the data center, which makes it easier to investigate and respond to a potential issue.

This rule must precede the next rule, which applies to all traffic so that you can log and monitor attempts to use unexpected applications on application-default ports regardless of the source after you first log violations from user zones.
To create this rule:

- The Source Zone includes all user zones and users.
- The Destination Zone is the data center web server tier (Web-Server-Tier-DC) at the data center perimeter.
- Set the Application to any and the Service to application-default so that the rule applies to all applications running on their standard ports.
- Set the Action to Drop to silently drop the traffic without sending a signal to the client or server.

STEP 2 | Block all applications from user zones on any port to identify applications running where they shouldn’t run.

This rule identifies legitimate, known applications that users are attempting to run on non-standard ports as well as unknown applications for which you may need to create custom applications. Investigate the source of any traffic that matches this rule to ensure that you aren’t allowing unknown-tcp, unknown-udp, or non-syn-tcp traffic. Be sure to place this rule after whitelist rules that allow traffic or this rule will block traffic that you intend to allow.

We will also create a different block rule later in this section that is similar to this rule (Unexpected-App-from-Any-Zone), except that it applies to traffic from any source, not just traffic from user zones. The reason for creating separate rules is that violations of the user-zone rule may indicate that a legitimate application which some users need to conduct business has not been designed correctly, so you may need to modify the application. Creating a separate rule for the rest of the traffic enables you to view separate logs for user traffic and for all other traffic attempting to enter the data center, which makes it easier to investigate and respond to a potential issue.

To create this rule:

- The Source Zone includes all user zones and users.
- The Destination Zone is the data center web server tier (Web-Server-Tier-DC) at the data center perimeter.
- Set the Application to any and the Service to any so that the rule applies to all applications running on any port.
- Set the Action to Drop to silently drop the traffic without sending a signal to the client or server.

STEP 3 | Blacklist applications designed to evade or bypass security, that attackers commonly exploit, or that are not necessary in the data center.
This rule protects the data center from applications that you know you don’t want on your network. Although the goal of a best practice security policy is positive enforcement using whitelist application rules, explicitly blocking and logging potentially dangerous application activity such as unsanctioned file sharing applications, remote access applications, or encrypted tunnels, provides visibility into and information about potential attacks. Even after you develop a solid application whitelist, keep this application blocking rule in the rulebase because logs from attempted violations help with investigations into potential attacks.

**Use this rule to block only applications you never want in your data center.**

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>Application</th>
<th>Service</th>
<th>URL Category</th>
<th>Action</th>
<th>Profile</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block-Bad-Appl</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Encrypted-Tunnels-AppFilter</td>
<td>any</td>
<td></td>
<td>Drop</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Filesharing-AppFilter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remoteaccess-AppFilter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DB-Server-Tier-DC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Engineering-DC-Infra</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Finance-DC-Infra</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IT Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SAP-Infra</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Web-Server-Tier-DC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To create this rule:

- Set the Source Zone, Address, and User to *any* because you’re blocking applications that nobody should be allowed to use in the data center.
- Specify all data center zones in the Destination Zone to protect all data center servers from bad applications.
- **Create an application filter** for each type (category) of application you want to block and specify any additional applications. This example includes application filters for encrypted tunnels, remote access, and file sharing. Block applications that you don’t use in the data center because there is no reason for that application traffic to be in the data center. The advantage of using application filters instead of application filters or listing individual applications is that filters are automatically updated, so you don’t need to maintain them as new applications come out.
- Set the Service to *any* to catch undesired applications on non-standard ports as well as default ports.
- Set the Action to Drop to silently drop the traffic without sending a signal to the client or server.

The application filters shown in the example rule are not a comprehensive list. Evaluate the application list you create based on How to Assess Your Data Center and add the applications you don’t want to allow to this rule. Place this blocking rule after the whitelist allow rules to allow exceptions to the rule. For example, IT needs to use remote access applications to manage data center devices, so you must allow that use of remote access applications before you block remote access applications for all other users. Another example is that you may sanction one or two file sharing applications in whitelist rules that precede this blacklist rule, and the application filter in this rule then blocks all the rest of those applications. If there are sets of applications or individual applications that you never want on your network and for which there are no exceptions, you can create a specific blacklist rule to block just those applications and place it at the top of the rulebase, above the application whitelist rules. However, if you do this, you must be certain that none of the blacklisted applications have legitimate business uses because they will be blocked.

**STEP 4** | Block all applications from any zone on the application-default port to identify unexpected applications.

This rule discovers applications from any zone that you didn’t know were running on your data center. Violations of this rule may indicate that an application has changed or may indicate a potential threat.
Monitor traffic that matches this rule to determine if it’s a potential threat or if you need to modify your whitelist application rules. Be sure to place this rule after whitelist rules that allow traffic or this rule will block traffic that you intend to allow, and after the rule in Step 1 so that it doesn’t catch traffic from user zones.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>Application</th>
<th>Service</th>
<th>Action</th>
<th>Profile</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unexpected-App-from-Any-Zone</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Web-Server-Tier-DC</td>
<td>any</td>
<td>any</td>
<td>application-default</td>
<td>Drop</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

To create this rule:

- The Source is any to cover all of the rest of the traffic attempting to enter the data center (the rule in Step 1 blocks and identifies unexpected user applications before traffic hits this rule).
- The Destination Zone is the data center web server tier (Web-Server-Tier-DC) at the data center perimeter.
- Set the Application to any and the Service to application-default so that the rule applies to all applications running on their standard ports.
- Set the Action to Drop to silently drop the traffic without sending a signal to the client or server.

**STEP 5** | Block all applications from any zone on any port to identify applications running where they shouldn’t run.

This rule identifies legitimate, known applications attempting to run on non-standard ports as well as unknown applications for which you may need to create custom applications. Investigate the source of any traffic that matches this rule to ensure that you aren’t allowing unknown-tcp, unknown-udp, or non-syn-tcp traffic. Be sure to place this rule after whitelist rules that allow traffic or this rule will block traffic that you intend to allow, and after the preceding rule so that it doesn’t catch traffic from user zones.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>Application</th>
<th>Service</th>
<th>Action</th>
<th>Profile</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unexpected-Any-Port</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Web-Server-Tier-DC</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Drop</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

To create this rule, use the same settings as in the rule Unexpected-App-from-User-Zone, except instead of specifying the user zones in the source, specify any zone to cover all of the rest of the traffic attempting to enter the data center, and set the Service to any to cover non-standard ports.

**STEP 6** | Discover unknown users attempting to run any application, on any port.

This rule identifies gaps in User-ID coverage by finding unknown users. It also identifies compromised or embedded devices in the user community that are trying to access your data center. (Embedded devices have no user interface, for example, printers, card readers, and cameras, but adversaries can compromise these devices and use them in an attack.)

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>Application</th>
<th>Service</th>
<th>Action</th>
<th>Profile</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover-Unknown-Users</td>
<td>any</td>
<td>any</td>
<td>unknown</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

This rule is almost the same as the interzone-default rule that prevents communication between zones (unless a whitelist rule allows the traffic), except instead of dropping traffic from all users, it only drops traffic from unknown users. This enables you to log rule matches separately and more easily investigate unknown users attempting to access your data center.
Define the Initial User-to-Data-Center Traffic Security Policy

Defining the initial best practice security policy for user traffic flowing to the data center begins the process of developing a data center application whitelist. The ultimate goal is to use positive security enforcement to protect your data center with a Zero Trust architecture by explicitly controlling who can access the data center, which data center applications they can access, and what resources they can access inside the data center. When you finish developing your best practice security policy, no unknown users should be able to access the data center and no unknown applications or resources should reside in the data center.

- **User-to-Data-Center Traffic Security Approaches**
- Create User-to-Data-Center Application Whitelist Rules
- Create User-to-Data-Center Authentication Policy Rules
- Create User-to-Data-Center Decryption Policy Rules

User-to-Data-Center Traffic Security Approaches

The traditional legacy approach to securing user traffic flowing to the data center leaves valuable assets exposed to risk, while the best practice approach protects your valuable assets.

<table>
<thead>
<tr>
<th>The Traditional Approach</th>
<th>Risk</th>
<th>The Best Practice Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based rules provide sufficient security because the data center is inside a trusted network.</td>
<td>Malicious applications access the network by spoofing port numbers, tunneling through a port, or using port hopping to avoid detection.</td>
<td>Application whitelist rules tie together applications, users, and servers so that only legitimate users using sanctioned applications can access the right sets of data center servers. <strong>When you transition from port-based to application-based rules, in the rulebase, place the application-based rule above the port-based rule it will replace. Reset the policy rule hit counter for both rules. If traffic hits the port-based rule, its policy rule hit count increases. Tune the application-based rule until no traffic hits the port-based rule for a period of time, then remove the port-based rule.</strong></td>
</tr>
<tr>
<td>Trust internal users and allow the application the user accesses to determine whether access is allowed based</td>
<td>An attacker gains access to a data center endpoint and then moves laterally to any other data center endpoint to exploit stolen credentials or server-side vulnerabilities. Unknown</td>
<td>Enable User-ID, block unknown users, and whitelist access for sanctioned users. Create separate identity domains for employees, partners, and contractors. Use multi-factor authentication (MFA) for partner, contractor, and sensitive server access.</td>
</tr>
</tbody>
</table>

---

**© 2019 Palo Alto Networks, Inc.**
The Traditional Approach | Risk | The Best Practice Approach
--- | --- | ---
on credentials and possibly on IP address rules. | users gain access to data center endpoints. | Send all unknown files to WildFire for analysis to identify new and unknown malware and protect against it.
Analyzing unknown files is unnecessary because the data center is inside a trusted network. | Users may inadvertently download malware from file sharing and other cloud applications. | The Palo Alto Networks suite of coordinated security tools works together to plug security holes and prevent attacks.
A mix of threat prevention profiles from multiple vendors. | A conglomeration of individual tools leaves security holes for attackers and may not work together well. | 

Create User-to-Data-Center Application Whitelist Rules

When you assess your data center, you gain the information to craft a set of application whitelist access rules based on purposeful decisions about who should have access to which applications running on which sets of servers. Craft the application whitelist security policy rules (Policies > Security) so that only the users you explicitly allow can use only the applications that pertain to their work on only the right sets of servers. Allow no unnecessary access, no unknown users, and no unknown applications.

- **Tag all sanctioned applications** with the predefined Sanctioned tag. Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.

Order the Data Center Security Policy Rulebase shows you how to order these rules with all of the other rules we create for the other three data center traffic flows and the block rules so that no rule shadows another rule.

- **To apply consistent security policy across multiple data centers, you can reuse templates and template stacks** so that the same policies apply to every data center. The templates use variables to apply device-specific values such as IP addresses, FQDNs, etc., while maintaining a global security policy and reducing the number of templates and template stacks you need to manage.

**STEP 1** | Enable the appropriate user access to your internal corporate DNS servers (don’t enable access to external DNS servers).

This rule restricts access to your corporate DNS servers, which reduces the attack surface and helps protect DNS entries about internal hosts and services. To avoid discovery by public DNS queries, DNS entries for internal corporate resources aren’t stored in publicly available DNS servers, so the only way an attacker can learn those entries is to compromise the corporate DNS server, so your DNS servers are attractive targets.

- **At the internet gateway (network perimeter), block all DNS traffic to public DNS servers. Do not allow DNS traffic to go out to the internet.**
This rule is an exception to the best practice of not allowing "any" user in policy rules because users need to access DNS services before they log in. This rule safeguards access to DNS services. To create this rule:

- Restrict access to the appropriate Destination Zone in the data center, **IT infrastructure**.
- Configure an address group for the **DNS Servers** and restrict access to only that group.
- Prevent access using any application except **dns**.
- Apply the full suite of Security Profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats. If an attacker hijacks your DNS server, the attacker can redirect traffic to phishing websites that look like the legitimate websites users are trying to access.
- Log DNS activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

**STEP 2 |** Allow the necessary IT personnel secured, privileged access to data center servers for management and maintenance.

This rule shows how to safeguard access to critical systems for users who have privileged accounts. Privileged accounts require a high level of trust and grant administrative access to critical systems that contain your company’s most valuable data, so you must tightly control and monitor privileged accounts. Leverage App-ID to specify only the applications IT users need to manage data center devices so that the firewall denies access for all other applications. In this example, a group of IT users needs administrative access to manage data center servers.

*IT privileged access for data center server management should be limited to management interfaces only, and should be on a dedicated VLAN so that server management traffic is separate from other traffic. The management interfaces should be on the same subnet. Don’t allow this type of access on data interfaces. If the IT group uses SSH or RDP for management access, don’t allow SSH or RDP access for other purposes.*

Your IT networking team’s organization determines whom to allow IT privileged access. For each type of privileged access, group servers and other devices by their access requirements. Allow only the necessary IT users to access each set of servers, using only applications required for device management.

To create this rule:

- Because only a subset of IT users may manage data center servers, leverage User-ID to create a group specifically for IT users who require that level of privileged access (in this example **pantac2012\IT-superusers**).
- Create a static address group (**IT-Server-Management**) that contains the management interface addresses of the servers you want the **pantac2012\IT-superusers** to manage and restrict the Destination to that address group in the **IT-server-access-DC** zone.
- Allow only the applications the IT superusers need to perform their business duties, on the default ports. In this example, the rule allows the **ssl**, **ssh**, and **ms-rdp** applications.
The allowed applications are examples. Allow the applications your IT department uses to manage data center servers. In some cases, applications over SSL may require the addition of the specific application to be identified correctly by App-ID.

- Attach the best practice security profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.
- Log activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

IT personnel also manage switches, routers, and other devices in the data center. If the same group of IT users manages those resources using the same applications, you can add them to the destination zone and address so that the rule allows IT superusers to access the management interfaces of those devices. If different IT user groups manage different sets of data center resources or use different applications, create separate, tight security policy rules for each user group and each set of applications.

Because user groups that have privileged accounts have access to critical systems, when you Create User-to-Data-Center Authentication Policy Rules, require MFA to prevent access if attackers compromise their credentials. Create corresponding authentication policy and decryption policy rules for each privileged access rule.

### STEP 3

| Allow access for employee user groups that have legitimate business reasons to communicate with data center servers. |

This rule shows how to limit each user group’s (or in some cases, an individual user’s) access to only the necessary applications and servers. For example, engineers need to access development servers in the data center. To create the security policy rule, create a dynamic address group that contains the IP addresses of all of the data center development servers that the group uses, identify the applications the engineers need to use on those servers, and construct the rule based on those groups.

To create this rule:

- Specify the engineering user groups that need access to engineering servers in the data center, in this example, pantac2012\apiusers and pantac2012\engg.
- Restrict access to the data center development servers by creating a dynamic address group (Dev-Servers) for them and setting it as the Destination Address.
- Restrict access to only the applications required for business purposes on the default ports.
- Attach the best practice security profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.
- Log activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

Use the same method to create granular whitelist access rules for each user group (if required, you can do this for individual users as well), so that each group can only use legitimate applications running on default ports to access only the sets of servers that they have business reasons to access. For example, allow only the group of Finance users who need access to servers that contain PCI to access those servers, using only the sanctioned finance applications required to accomplish business goals.
Similar to the whitelist rule for engineering user access to data center servers, this rule allows users in the pantac2012\finance-users and pantac2012\accounting-users groups to use only the specified applications to access only the servers in the Fin-Servers dynamic address group. The rule applies the best practice security profiles to allowed traffic and logs activity.

**STEP 4 | Allow targeted, limited data center access to contractors, partners, customers, and other third-parties.**

This rule shows how to tightly control access for third-party users so that they can use only the applications they need on only the servers they need. For example, a company hires a group of SAP developer contractors. The SAP developers need to access the SAP database in the data center and make SQL queries. However, SQL also runs on production databases that the SAP developers should not access. The company needs to control three access vectors:

- **User group**—SAP developer contractors.
- **Applications**—MS-SQL and SAP.
- **Servers**—SAP database servers only. Deny all other data center server access.

The combination of User-ID to isolate the SAP contractor user group, App-ID to limit the group to using only the necessary applications, and a dynamic address group that limits access to only the SAP database servers in the data center enables the company to provide exactly the access the SAP contractors need to perform their duties, but no more.

To create this rule:

- Specify the Source Zone and User to limit access to users in the pantac\sap-contractors group coming from the Contractors zone.
- Restrict the Destination to the SAP database servers (SAP DB Server dynamic address group) in the SAP-Infra zone.
- Allow the SAP contractors to use only the applications they need to perform their business duties, on the default ports. In this example, the rule allows the ms-sql-analysis-service, mssql-db, mssql-mon, and sap applications.
- Attach the best practice security profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.
- Log activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

Granular whitelist security policy rules prevent all but the access required for business purposes and reduce risk by reducing the attack surface. Create similar whitelist rules for each third-party group that requires access to your data center.

Instead of trusting third-party users and companies to secure their credentials, require multi-factor authentication (MFA; Create User-to-Data-Center Authentication Policy Rules) to prevent access if attackers steal credentials or otherwise compromise third-party systems. MFA authentication would have prevented several high-profile data breaches that occurred over the past several years.
Verify that only the applications you explicitly whitelisted in the security policy rules are running by viewing the predefined Applications report (Monitor > Reports > Application Reports > Applications). If you see unexpected applications in the report, review the application whitelist rules and refine them so that they don’t allow the unexpected applications.

Create User-to-Data-Center Authentication Policy Rules

Authentication Policy rules force users to prove that they are who they claim to be before they can access data center services, applications, and other resources. Authentication is especially important for protecting your most valuable assets because if an attacker steals credentials and authenticates with the firewall, the attacker may be able to access and compromise any asset in your data center.

For access to sensitive servers and for third-party user access to servers (for example, SAP development contractors accessing SAP servers in the data center), implement Multi-Factor Authentication (MFA) to prevent attackers from using stolen credentials to access those systems. An Authentication policy with MFA would have prevented a number of successful high-profile breaches over the past several years.

Before you create Authentication Policy rules (Policies > Authentication), you must configure Authentication Policy dependencies to tie the authentication method, the authentication type, how to access the authentication server, and the use of Captive Portal to an Authentication Policy rule that specifies who can authenticate on which servers using what services.

STEP 1 Authenticate employee user groups and individuals that have legitimate business reasons to use data center servers.

This rule show how to authenticate user groups so that they can access services required for their business activities on the necessary servers. For example, engineers need to authenticate before they can access development servers and applications.

To create this rule:

- Specify the engineering user groups that need to authenticate before they can access engineering servers in the data center, in this example, pantac2012\apiusers and pantac2012\engg.
- Apply authentication for these user groups to data center development server access requests by creating a dynamic address group (Dev-Servers) for them and setting it as the Destination Address.
- Apply the Authentication rule to the services engineering groups need to use for business purposes, in this example Perforce, rdp, service-http, service-https, and ssh (developers may need to use SSH and RDP to access Linux servers and should authenticate before being allowed to access those servers). The services in your authentication rules depend on the services that the groups need to use.
- Configure an Authentication Enforcement Object (Auth-Dev-Servers) that specifies the authentication method and the Authentication Profile and add it to the rule.
- Log activity so that you can track and analyze rule violations, which may indicate an attempted attack.

Another authentication use case is when a group requires access to a particular set of services. For example, Finance Department users need access to sensitive Payment Card Information (PCI) using particular services and should authenticate before being granted access. To authenticate users for those
services, this rule uses a custom Service Group (Objects > Service Groups) that includes only services for which the firewall should authenticate Finance users.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Source Zone</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination User</th>
<th>Service</th>
<th>Authentication Enforcement</th>
<th>Log Settings</th>
</tr>
</thead>
</table>

To create this rule:

- Specify the user groups that need to authenticate before they can access finance servers in the data center, in this example, pantac2012\accounting-users and pantac2012\finance-users.
- Apply authentication for these user groups to data center finance server access requests by creating a dynamic address group (Finance-DC-Infra) for them and setting it as the Destination Address.
- Apply the authentication rule to the services that Finance users need to use for business purposes, in this example service-http, service-https, and the services defined in the custom service group Custom-Finance-Srvrs-Services, so that users must authenticate before they can access these services.
- Configure an Authentication Enforcement Object (Auth-Finance-Servers) that specifies the authentication method and the Authentication Profile and add it to the rule.
- Log activity so that you can track and analyze rule violations, which may indicate an attempted attack.

**STEP 2 |** Authenticate contractors, partners, customers, and other non-employee groups that require data center access.

This rule requires MFA for third-party user groups such as contractors, partners, and customers because you have less control over the business and security practices of their companies and personnel than you do over your employees. Requiring these users to authenticate with at least two factors protects your data center against credential theft at a third-party company.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Source Zone</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination User</th>
<th>Service</th>
<th>Authentication Enforcement</th>
<th>Log Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Resources</td>
<td>Group Users</td>
<td>User to DC-IP</td>
<td>Contractors</td>
<td>SAP-Infra</td>
<td>SAP DB Servers</td>
<td>SAP-Services</td>
<td>Auth-SAP-Servers</td>
<td>Log Authentication Timeouts: yes Log Forwarding: MFA</td>
</tr>
</tbody>
</table>

To create this rule:

- Specify the contractor user groups that need to authenticate before they can access SAP servers, in this example, the pantac\sap-contractors group.
- Apply authentication for these users to the SAP database servers by creating a dynamic address group (SAP DB Server) for them and setting it as the Destination Address.
- Apply the Authentication rule to the services SAP contractors need to use for business purposes. Create a custom service group (Sap-Services) to define the ports on which SAP contractors can authenticate and add other necessary services, in this example, service-http and service-https.
- Configure an Authentication Enforcement Object (Auth-SAP-Servers) that specifies the authentication method and the Authentication Profile and add it to the rule. In this case, the authentication type must be one that supports MFA, and you must Add an MFA server profile to the Authentication Profile (Factors tab) and perform the rest of the steps to configure MFA.
- Log activity so that you can track and analyze rule violations, which may indicate an attempted attack.
STEP 3 | Authenticate users who need specialized access, such as IT personnel who need secured access to data center servers for management and maintenance.

This rule shows you how to configure authentication for users who have privileged accounts, which grant administrative access to critical systems. Because compromising the credentials of a privileged user hands an attacker the keys to your data center kingdom and its valuable assets, you need to protect against stolen credentials by requiring at least two factors of authentication to ensure that only legitimate users are granted access. This example shows how to authenticate the right IT users for access to data center server management interfaces.

To create this rule:

- Specify the privileged account users who need to authenticate before they can access data center server management interfaces, in this example, the pantac\it-superusers group.
- Apply authentication for the user group to data center management interface access requests by creating a dynamic address group (IT-Server-Management static address group) for them and setting it as the Destination Address.
- Apply the Authentication rule to the services privileged IT personnel need to use for business purposes, in this example, the custom service group Custom-IT-ports, which identifies all of the server management ports (which should be placed on the same subnet).
- Configure and apply an Authentication Enforcement Object (Auth-IT-Server-Mgmt in this example) that enforces requiring MFA (two factors) for authentication. Add an MFA server profile to the Authentication Profile (Factors tab) and perform the rest of the steps to configure MFA. Using MFA is critical because you need to be certain of the identity of each IT user who has a privileged account since they have access to device management.

To further reduce the opportunity for an attacker to compromise the data center using stolen credentials or an opportune moment when a workstation is unattended but not locked, when you configure MFA, configure authentication timestamps for the authentication factors. With valuable data center assets, it's best to prioritize securing services and applications.

- Log activity so that you can track and analyze rule violations.

IT personnel also manage switches, routers, and other devices in the data center. If the same group of IT users manages those resources, you can add them to the destination zone and address so that the rule authenticates IT superusers before they can access the management interfaces of those devices. If different IT user groups manage different sets of data center resources, create separate, tight security policy rules and corresponding authentication policy and decryption policy rules for each user group.

Do not send credentials in cleartext. For example, if you use RADIUS, use a supported EAP method to transport credentials securely inside TLS.

Create User-to-Data-Center Decryption Policy Rules

Create Decryption policy rules for traffic that enters the data center from the user population to provide visibility so that you can inspect the traffic and safeguard your most valuable assets. When you create a Security policy rule that allows a group of users (or a particular user) access to a set of data center servers, create a decryption policy rule to decrypt that traffic.

Because the data center houses your most valuable assets, decrypt all the data center traffic you can decrypt. Start by decrypting traffic to the most critical servers, decrypting high-risk traffic categories, and decrypting traffic from the least trusted network segments (for example, prioritize decrypting third-party
traffic from partners, customers, or contractors over decrypting traffic from a trusted internal segment), and then expand the effort until you have applied decryption to traffic destined to all of your data center assets. Decrypt as much traffic as you can while retaining acceptable performance.

**Exclude Unsuitable Traffic from Data Center Decryption.** Regulations and compliance over personal information differ from country to country and even within country regions. Different companies may have different compliance rules about personal information. Decrypt as much traffic as you can, but if your data center houses information that regulations or company rules exempt from decryption, don’t decrypt that traffic.

In Create User-to-Data-Center Application Whitelist Rules, we created Security policy rules that allow DNS access, allow engineering users to access engineering development servers, allow SAP contractor developers to access only the SAP development servers, and allow a particular set of IT users data center server management access. Here we create decryption policy rules (Policies > Decryption) to decrypt the traffic that these rules allow.

The decryption policy rules share some common elements in regard to these traffic flows:

- When you create a Decryption policy rule, the objective is to decrypt traffic so that a Security policy rule can examine it and allow or block it based on policy. To accomplish that, the Decryption policy rule must use the same source zone(s) and user(s) as the analogous security policy rule, and the same destination zone and address (often defined by a dynamic address group so that as you add or remove servers, you can update the firewall without a commit operation). Defining the same source and destination in the Security policy and in the Decryption policy applies both policies to the same traffic.
- The Action for all of these rules is decrypt, except in the case of sensitive personal information as shown in Step 4.
- The decryption rules that use SSL Inbound Inspection to examine incoming traffic require the appropriate server certificate.
- All of these decryption rules use the Best Practice data center decryption profile shown in Create the Data Center Best Practice Decryption Profiles.

**STEP 1 | Decrypt allowed traffic from employee user groups to data center servers.**

This rule shows how to decrypt traffic from a user group to the data center servers that the group is allowed to access to provide visibility into that traffic. For example, the application whitelist rules we created include a Security policy rule that allows engineering users to access development servers in the data center. To protect the development servers, decrypt incoming traffic so that the firewall can inspect it and apply threat prevention profiles.

To create this rule:

- Specify the same source and destination as in the analogous security policy rule. In this case, the Source users are the pantac\apiusers and pantac\engg user groups in the Engineering-Users zone, and the Destination is the servers specified in the Dev-Servers dynamic address group in the Engineering-DC-Infra zone.
- On the Options tab, set the Action to Decrypt and the decryption Type to SSL Inbound Inspection. Specify the server certificate for the development servers (DevServers) and apply the data center best practice Decryption Profile to apply SSL Inbound Inspection and SSL Protocol Settings to the traffic.
Create a similar Decryption policy rule for allowed data center traffic of each user group (or individual user, if applicable) based on the source zone and user group (or user) and on the destination zone and server group (as defined by the dynamic address group membership).

**STEP 2 | Decrypt allowed traffic from contractors, partners, customers, and other third-parties.**

This rule shows how to decrypt from third-party groups to the data center servers they are allowed to access. For example, the whitelist rules include a security policy rule that allows limited access for SAP developer contractors to SAP database servers in the data center. Decrypt incoming traffic so that the firewall can inspect it, apply threat prevention profiles to it, and protect the SAP data center servers.

To create this rule:

- Specify the same source and destination of the traffic to decrypt as in the analogous security policy rule. In this case, the Source users are the `pantac\sap-contractors` user group in the Contractors zone, and the Destination is the servers specified in the SAP DB Servers dynamic address group in the SAP-Infra zone.
- On the Options tab, set the Action to Decrypt and the decryption Type to SSL Inbound Inspection. Specify the server certificate for the development servers (`SAP Server Cert`) and apply the data center best practice Decryption Profile to apply SSL Inbound Inspection and SSL Protocol Settings to the traffic.

Create a similar Decryption policy rule for each third-party group's allowed data center traffic based on the source zone and user group and the destination zone and server group (as defined by the dynamic address group membership).

**STEP 3 | Decrypt privileged allowed access to data center servers (except traffic pertaining to personal information if regulations or compliance rules prohibit it).**

This rule shows how to decrypt traffic for privileged access because you should decrypt as much traffic as possible to provide the visibility necessary to defend the data center, no matter how much you trust the users. If you don't decrypt allowed traffic, you can't apply threat prevention profiles, and if the traffic conceals malware or other threats, you won't see them. This example references the Security Policy whitelist rule we created previously to provide management interface access to data center servers for IT superusers.

*If the IT group that manages and maintains data center servers uses SSH, you can’t decrypt the SSH traffic. You can configure SSH Proxy to block SSH tunnels and prevent SSH from tunneling potentially malicious content and applications. If the IT group uses SSL, create a Decryption Policy rule using SSL Forward Proxy instead of SSL Inbound Inspection. The reason is that SSL Inbound Inspection requires the server certificate to perform decryption. Because IT manages many data center servers, creating SSL Inbound Inspection rules for each server is onerous and difficult to manage. SSL Forward Proxy decryption scales better in this use case.*

The following example shows the Decryption policy rule for the SSL Forward Proxy use case.

To create this rule:
• Specify the same source and destination of the traffic to decrypt as in the analogous security policy rule. In this case, the Source users are the pantac\it-superusers user group in the IT-Users zone, and the Destination is the servers specified in the IT-Server-Management static address group in the IT-server-access-DC zone.

• On the Options tab, set the Action to Decrypt and the decryption Type to SSL Forward Proxy. Apply the data center best practice Decryption Profile to apply SSL Forward Proxy and SSL Protocol Settings to the traffic.

If other groups require privileged access, create a similar type of Decryption Policy rule for each group.

IT personnel also manage switches, routers, and other devices in the data center. If the same group of IT users manages those resources, you can add them to the destination zone and address so that the rule decrypts traffic for connections to the management interfaces of those devices. If different IT user groups manage different sets of data center resources, create separate, tight security policy rules and corresponding decryption and authentication policy rules for each user group.

The next example shows the Decryption policy rule for the SSH Proxy use case. You may also choose not to decrypt the traffic instead of using SSH Proxy decryption.

To create this rule:

• The traffic source and destination are the same as for the preceding SSL Forward Proxy use case example rule.

• On the Options tab, set the Action to Decrypt and the decryption Type to SSH Proxy. Apply the data center best practice Decryption Profile to apply SSH Proxy and SSL Protocol Settings to the traffic.

IT personnel also manage data center switches, routers, and other devices. If the same group of IT users manages those resources, you can add them to the destination zone and address so that the rule decrypts traffic for connections to the management interfaces of those devices. If different IT user groups manage different sets of data center resources, create separate, tight security policy rules and corresponding decryption and authentication policy rules for each user group.

STEP 4 | Do not decrypt sensitive personal information if prohibited by regulations or compliance rules.

This rule shows how to create a policy-based decryption exclusion if you need to except traffic from decryption for regulatory or compliance reasons. This example references the Security Policy whitelist rule we created previously to provide Finance server access for Finance users. If regulations or compliance permit you to decrypt this traffic, decrypt it so that the firewall can see the traffic and protect against threats.

To create this rule:

• Specify the same source and destination of the traffic to decrypt as in the analogous security policy rule. In this case, the Source users are the pantac2012\accounting-users and pantac2012\finance-users user groups in the Finance-Users zone, and the Destination is the servers specified in the Finance-Servers dynamic address group in the Finance-DC-Infra zone.

• On the Options tab, set the Action to No Decrypt and the decryption Type to SSL Forward Proxy so that the firewall won’t ask for a server certificate. Apply the data center best practice Decryption Profile to apply No Decryption and SSL Protocol Settings to the traffic.
Define the Initial Internet-to-Data-Center Traffic Security Policy

As with the other data center traffic flows, tightly control traffic flowing from the internet to the data center with application whitelist security policy rules so that no traffic using unknown or unsanctioned applications can enter the data center. In addition, protect the data center web servers from denial-of-service (DoS) attacks by applying DoS Protection policy rules (with DoS Protection profiles) to external traffic destined for the data center web server tier.

- Internet-to-Data-Center Traffic Security Approach
- Create Internet-to-Data-Center Application Whitelist Rules
- Create Internet-to-Data-Center DoS Protection Policy Rules
- Create Internet-to-Data-Center Decryption Policy Rules

Internet-to-Data-Center Traffic Security Approach

The traditional legacy approach to securing data center traffic flowing to the data center from the internet leaves valuable assets exposed to risk, while the best practice approach protects your valuable assets. The major risks from traffic entering the data center are inadvertently downloading malware from an infected external server or inadvertently placing malware on an external server from a compromised data center server.

<table>
<thead>
<tr>
<th>The Traditional Approach</th>
<th>Risk</th>
<th>The Best Practice Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create port-based security policy.</td>
<td>Malicious applications access the network by spoofing port numbers, tunneling through a port, or using port hopping to avoid detection.</td>
<td>Application whitelist rules prevent applications from running on non-standard ports. Log and monitor whitelist violations.</td>
</tr>
</tbody>
</table>

When you transition from port-based to application-based rules, in the rulebase, place the application-based rule above the port-based rule it will replace. Reset the policy rule hit counter for both rules. If traffic hits the port-based rule, its policy rule hit count increases. Tune the application-based rule until no traffic hits the port-based rule for a period of time, then remove the port-based rule.

An Intrusion Prevention System (IPS) is often deployed as an An IPS is an in-band detection and prevention system, while an IDS is an out-of-band detection system. Deploying an IPS as an IDS takes In-band on the firewall, use Palo Alto Networks App-ID, User-ID, and Content-ID to create application whitelist security policies that tightly control access. Apply
The Traditional Approach | Risk | The Best Practice Approach
---|---|---
Intrusion Detection System (IDS). | intrusion detection out of the direct communication path between the source and the destination, so real-time prevention can’t occur and threats can enter the data center. | the security profiles to stop known and new threats.

A web application firewall is sufficient to protect the data center. | An attacker places command-and-control (C2) software onto a compromised data center endpoint, opening the network to attack and potentially serving client-side exploits in a watering-hole attack. | Stop attackers from placing C2 software on data center endpoints simply by assigning the strict Anti-Spyware security profile to the security policy rule that controls the traffic. This profile is one of the firewall’s included features, so it costs you nothing extra to apply this protection.

Create Internet-to-Data-Center Application Whitelist Rules

The greatest risks from traffic entering the data center from the internet are inadvertently downloading malware from an infected external client or inadvertently placing malware on an external server if a client pulls data from a compromised server in your data center. Protect traffic from the internet to the data center so that you don’t inadvertently download malware that takes advantage of server vulnerabilities or allow a client to download malware from one of your company’s servers that could infect partners, customers, or wind up on a website used by your industry (serving a watering-hole attack).

Ensure that the source of traffic to the data center doesn’t come from malicious IP addresses or other potentially risky sources, and only allow applications required for business purposes. Don’t allow unnecessary (and especially unknown) applications in the data center. To do these things:

- Create whitelist rules that control the sanctioned and allowed applications that external devices can use to communicate with your data center.

  ![Tip](image)
  
  **Tag all sanctioned applications with the predefined Sanctioned tag.** Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.

- Create an External Dynamic List to identify bad IP addresses and use it to prevent them from accessing your data center.

- Create a custom application for any proprietary application so that you can identify the application and apply security to it.

If you have existing Application Override policies that you created solely to define custom session timeouts for a set of ports, convert the existing Application Override policies to application-based policies by configuring service-based session timeouts to maintain the custom timeout for each application and then migrating the rule the an application-based rule. Application Override policies are port-based. When you use Application Override policies to maintain custom session timeouts for a set of ports, you lose application visibility into those flows, so you neither know nor control which applications use the ports. Service-based session timeouts achieve custom timeouts while also maintaining application visibility.

- Apply the full suite of Security Profiles to allow rules to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.

- Log all allowed traffic.
Order the Data Center Security Policy Rulebase shows you how to order these rules with all of the other rules we create for the other three data center traffic flows and the block rules so that no rule shadows another rule.

To apply consistent security policy across multiple data centers, you can reuse templates and template stacks so that the same policies apply to every data center. The templates use variables to apply device-specific values such as IP addresses, FQDNs, etc., while maintaining a global security policy and reducing the number of templates and template stacks you need to manage.

Allow sanctioned application traffic from vendors, contractors, and customers, restricted to only the necessary applications.

This rule shows how to secure application traffic arriving at the data center from external sources by tightly controlling the allowed application(s), allowing them only on the default port, and blocking sources that you know are bad using an External Dynamic List to identify known bad IP addresses.

To create this rule:

- Prevent known bad sources from attempting to access the data center. Use the Negate option in the Security Policy rule Source Address to block connections from bad IP addresses. This example uses an External Dynamic List (Bad IPs List) to identify known bad IP addresses and block them. (The strikethrough text in the source address indicates that it is negated rather than allowed.)
- Restrict the application(s) to only the application(s) required for business purposes and allow them to run only on their default ports (application-default) to prevent evasive malware from attempting to run on non-standard ports. In this example, the vendor uses a proprietary application called Acme. We created a custom application to identify the Acme proprietary application so that the firewall can classify the traffic and apply the appropriate Security policy.
- Restrict the destination for Acme application traffic to the Web-Servers dynamic address group in the Web-Server-Tier-DC zone. If the destination address isn't in the web server tier, the firewall drops the traffic.

Verify that only the applications you explicitly whitelisted in the security policy rules are running by viewing the predefined Applications report (Monitor > Reports > Application Reports > Applications). If you see unexpected applications in the report, review the application whitelist rules and refine them so that they don't allow the unexpected applications.

Create Internet-to-Data-Center Decryption Policy Rules

Create Decryption policy rules to provide visibility into traffic that enters the data center from the internet so that you can apply Security policy to that traffic. When you create a Security policy rule that allows access to a set of data center servers, create a decryption policy rule to decrypt that traffic. In Create Internet-to-Data-Center Application Whitelist Rules, we created a Security policy rule that allows access from internet to the web server tier in the data center, using only whitelisted applications. Here we create a decryption policy rule (Policies > Decryption) to decrypt the traffic that this rule allows.

To decrypt traffic so that a Security policy rule can examine it and allow or block it based on policy, the Decryption policy rule must use the same source zone(s) and user(s) as the analogous security policy rule, and the same destination zone and address (often defined by a dynamic address group) so that as you add
or remove servers, you can update the firewall without a commit operation). Defining the same source and destination in the Security policy and in the Decryption policy applies both policies to the same traffic.

The decryption rule uses the Best Practice data center decryption profile shown in Create the Data Center Best Practice Decryption Profiles.

**STEP 1** Decrypt allowed traffic from the internet to data center web servers.

This rule shows how to decrypt traffic from externally initiated connections to the data center. For example, the application whitelist rules we created allow external traffic access to the data center web servers, using only certain applications. To protect the data center web servers, decrypt traffic so the firewall can inspect it and apply threat prevention profiles.

To create this rule:

- Specify the same source and destination as in the analogous security policy rule. In this case, the Source is the L3-External zone, and the Destination is the servers specified in the Web-Servers dynamic address group in the Web-Server-Tier-DC zone.
- On the Options tab, set the Action to Decrypt and the decryption Type to SSL Inbound Inspection. Specify the server certificate for the web servers (Web Server Cert) and apply the data center best practice Decryption Profile to apply SSL Inbound Inspection and SSL Protocol Settings to the traffic.

**STEP 2** Create similar Decryption policy rules for traffic from the internet to any other server group, if such access is allowed, and for the other applications you allow.

**Create Internet-to-Data-Center DoS Protection Policy Rules**

One method attackers use to disrupt a network is a Denial-of-Service (DoS) attack intended to overwhelm targeted systems that are connected to the internet, take them down, and make them unavailable to all of your legitimate users and services. Data center web servers are an attractive target because taking them down prevents most legitimate access to the data center.

Protect the data center web server tier by applying a classified DoS Protection Policy to internet traffic destined for those servers. A classified DoS Protection policy applies a classified DoS Protection Profile that controls the number of incoming connections to the traffic defined in the policy.

In addition, configure packet buffer protection for each zone to protect the firewall from single-session DOS attacks that can overwhelm the firewall’s packet buffer and cause legitimate traffic to drop, especially on firewalls that protect critical services.

**STEP 1** Create a classified DoS Protection Profile that protects data center web servers from DoS attacks by limiting the number of connections-per-second to prevent a SYN flood attack.

This DoS Protection profile limits the number of connections-per-second (CPS) for the traffic defined in the DoS Protection Policy rules to which you attach the profile, to prevent a DoS attack from taking down your web servers. The profile sets progressive CPS thresholds to alert you, to activate Random Early Drop (RED) packet drop, and to block new connections, as well as a duration during which new connections remain blocked. The CPS thresholds you configure to protect your data center web servers depends on the capacity of your web servers.
To create this profile:

- Name the profile, select Classified as the profile Type, set the CPS values to alert (Alarm Rate), activate RED (Activate Rate), begin blocking new sessions (Max Rate), and set the amount of time in seconds to block new sessions (Block Duration) when the CPS rate reaches the Max Rate threshold.

If you don’t use protocols such as UDP or other IP protocols, restrict them using a combination of Security policy rules to whitelist applications and Zone Protection Profiles to block unused protocols by setting flood protection CPS to zero packets for protocols you want to block.

STEP 2 | Create a classified DoS Protection policy rule to define the servers you want to protect from a DoS attack and attach the DoS Protection profile to it.

This rule prevents a SYN flood attack from taking down your data center web server tier. This example applies the classified DoS Protection profile to external traffic allowed to connect to the web server tier.

To create this rule:

- To apply DoS protection to traffic destined for the web server tier, the DoS Protection policy must apply to the same traffic as the Security Policy rule that allows the traffic. In this example, this DoS rule protects the traffic we allowed in Create Internet-to-Data-Center Application Whitelist Rules.
- On the Option/Protection tab, specify the web services (service-http and service-https), set the Action to protect to apply the DoS Protection profile's SYN flood thresholds to the traffic, set the Log Forwarding method (assuming that you have configured log forwarding), and select the classified DoS Protection profile we configured for the traffic in the preceding step (Internet to DC).

To protect against SYN flood attacks from internal sources, create a separate DoS Protection policy rule that specifies your internal zones as the source zone instead of L3-External. Creating separate rules for external and internal attack sources provides separate reporting that makes investigating attack attempts easier.
Define the Initial Data-Center-to-Internet Traffic Security Policy

Depending on your data center architecture, servers in the data center may reach out to the internet to retrieve software updates or to check server certificate revocation status. The data center is a great place for adversaries to hide because security plans often focus on user communication and overlook servers that communicate with the internet. When data center servers initiate communication directly with the internet, you need to protect against several security risks:

- **Data exfiltration**—Attackers use legitimate applications such as FTP or HTTP, or other methods such as DNS tunneling, to steal data. Create an application whitelister security policy rule that allows only the applications required for server updates so that all other applications are blocked, even if they are legitimate applications in other circumstances. Loose application rules present opportunities to attackers.

- **Command-and-control (C2) using legitimate applications**—If data center servers are allowed to communicate with the internet using legitimate applications that are not for software updates, attackers could use those otherwise legitimate applications for C2 activities. For example, allowing web-browsing on non-standard ports creates opportunities for attackers. Servers should only be allowed to communicate with the internet using only the specific applications required for software updates on their default ports, and no other applications, even if those applications are legitimate and sanctioned for other uses.

- **Downloading additional malware**—If an attacker compromises a data center server, the malware on the server may download more malware from the internet through a phone-home or other mechanism. A strict whitelist rule that allows communication only with the appropriate update servers using only the necessary update applications prevents attackers from contacting websites that house malware and from exfiltrating data. In addition, install Traps on the data center servers (and all of your endpoints) to prevent malware that already resides on a server from executing.

- **Data-Center-to-Internet Traffic Security Approaches**
  - Create Data-Center-to-Internet Application Whitelist Rules
  - Create Data-Center-to-Internet Decryption Policy Rules

### Data-Center-to-Internet Traffic Security Approaches

The traditional legacy approach to securing data center traffic flowing to the internet leaves valuable assets exposed to risk, while the best practice approach protects your valuable assets.

<table>
<thead>
<tr>
<th>The Traditional Approach</th>
<th>Risk</th>
<th>The Best Practice Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create port-based rules and/or IP-based rules, which provide sufficient security in the trusted network.</td>
<td>Port-based and IP-based rules can’t control which applications to allow to connect to the internet. If a port is open, any application can use the port.</td>
<td>Create strict application-based whitelister rules that allow only data center servers that retrieve updates to use only legitimate applications to communicate only with legitimate update servers. Log and monitor whitelist rule violations.</td>
</tr>
</tbody>
</table>

*When you transition from port-based to application-based rules, in the rulebase, place the application-based rule above the port-based*
<table>
<thead>
<tr>
<th>The Traditional Approach</th>
<th>Risk</th>
<th>The Best Practice Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data center servers only reach out to trusted servers such as update servers, so decrypting that traffic isn’t necessary.</strong></td>
<td><strong>Malware or command-and-control software that is already in the data center may attempt to communicate with external servers to download more malware or exfiltrate data.</strong></td>
<td><strong>Decrypt all traffic from the data center to the internet. Create a custom URL categories that defines the URLs data center servers are allowed to contact and use it in Security policy to limit internet access to external servers. Use the same custom URL in Decryption policy to decrypt traffic to those external servers.</strong></td>
</tr>
<tr>
<td><strong>Mix blocking and alerting threat prevention profiles from multiple vendors.</strong></td>
<td><strong>A conglomeration of individual tools leaves security holes for attackers and may not work together well.</strong></td>
<td><strong>The Palo Alto Networks suite of coordinated security tools works together to plug security holes and prevent attacks.</strong></td>
</tr>
</tbody>
</table>

Create Data-Center-to-Internet Application Whitelist Rules

The main use case for data center servers initiating connections to external servers on the internet is to update software or to obtain certificate status. The greatest risk is connecting to the wrong server, especially for Linux updates because there are many third-party URLs to which you may inadvertently connect. Ensure that your data center servers receive updates from legitimate update servers, using only the required applications on their default ports.

To do this, create strict application whitelist rules that limit the external servers to which data center servers connect and the applications that data center servers use when connecting to external servers. **Tag all sanctioned applications** with the predefined **Sanctioned tag.** (Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.) A strict application whitelist disrupts potential attacks by:

- Preventing malware that is already on a data center server from connecting to a compromised external server (**phoning home**) and downloading additional data because the whitelist rules don’t allow connections to those servers.
- Preventing attackers from using legitimate applications such as FTP, HTTP, or DNS tunneling to exfiltrate data or using legitimate applications such as web-browsing on non-standard ports for command-and-control (C2) operations because the whitelist rules don’t allow data center servers to communicate with the internet using those applications. An additional way to help prevent exfiltration is to use the File Blocking profile’s **Direction** control to block outbound update files so you only allow downloading for software update files.
Create a strict whitelist rule for each application that requires software updates from a different set of external servers. In many cases, App-ID alone isn’t enough to protect data center servers. For example, for Linux server updates, it’s not enough to limit traffic to an update application such as `yum` or `apt-get` because that doesn’t prevent connecting to illegitimate servers. The best practice is to find the URLs that data center servers need to connect to, create custom URL categories (Objects > Custom Objects > URL Category) that specify the websites to use, and combine them with App-ID in Security policy rules. The combination of App-ID and custom URL categories locks down the external servers with which the data center servers can connect by preventing the use of illegitimate applications and preventing connections to update servers that aren’t in the custom URL category. For example, in a Security policy rule that allows data center servers to connect to CentOS update servers, you could create a custom URL category called `CentOS-Update-Servers` and add the CentOS update sites your servers use to the custom category.

To find out the URLs of legitimate Linux update servers and other update servers, work with software engineering, development operations, and other groups that update software to understand where they go to get updates. You can also log web browsing sessions, collect the URLs to which developers connect, and then take the URLs to engineering to filter out the right URLs for the Security policy.

Don’t use the URL Filtering Profile (PAN-DB URL Filtering) in Security policy rules for data center servers that communicate with the internet because you don’t want to allow all update servers. Restrict communication so that data center servers only reach out to the particular servers from which they retrieve updates.

In addition, all allowed communication should occur on the standard ports for each application. No applications should run on non-standard ports. As with all data center traffic, monitor whitelist violations because violations indicate either that you need to update the security policy to allow legitimate traffic or that an adversary is in or is attempting to enter the network.

Order the Data Center Security Policy Rulebase shows you how to order these rules with all of the other rules we create for the other three data center traffic flows and the block rules so that no rule shadows another rule.

To apply consistent security policy across multiple data centers, you can reuse templates and template stacks so that the same policies apply to every data center. The templates use variables to apply device-specific values such as IP addresses, FQDNs, etc., while maintaining a global security policy and reducing the number of templates and template stacks you need to manage.

**STEP 1 | Allow data center servers to access software update servers.**

This rule shows how to restrict access to software update servers on the internet so that data center servers communicate only with legitimate, known servers and don’t communication with other external update servers. This example allows engineering data center servers to access CentOS update servers and restricts communication to using only the necessary applications to establish connections to only the right set of update servers.

To create this rule:
- Restrict the source of CentOS update requests to only the data center servers that need to retrieve updates, in this example the `Dev-Servers` dynamic address group in the `Engineering-DC-Infra` zone.
• Restrict the application(s) that data center servers can use to communicate with external update servers to only the required application(s), in this example, yum for CentOS updates. Only allow the application(s) to run on the default port to prevent evasive malware from attempting to use non-standard ports.

• Create a custom URL category to define the URLs of the update servers to which the data center servers can connect. In this example, the CentOS-Update-Servers custom URL category defines the update server URLs that the data center servers can reach.

• Apply the full suite of Security Profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.

• Log update activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

This combination of restrictions also prevents attackers who have already compromised a data center server from reaching other destinations and using other applications to exfiltrate data or download additional malware.

Similarly, a rule allowing the same servers to communicate with Microsoft Windows update servers uses the same construction.

In addition to applying the best practice security profiles and logging traffic that this rule allows, the source zone and address are the same as in the preceding CentOS update rule. The differences are:

• The applications pertain to Microsoft updates. In addition to the ms-update application, Microsoft updates require the ssl application because ms-update depends on SSL. As with the CentOS update rule, only standard ports are valid.

  Some applications have dependencies on other applications. For a given application, you must allow all dependent applications or the application won’t work. You can filter applications (Objects > Applications) to find application dependencies. For example, to find the SSL dependency for the ms-update application, filter on ms-update, click ms-update, and check the Depends on: field.

• The custom URL category (Win-Update-Servers) contains the URL for Windows updates so that contact with other URLs is denied.

STEP 2 | Allow data center servers to access DNS and NTP update servers.

This rule shows how to restrict access to DNS and NTP update servers on the internet so that data center servers communicate only with legitimate, known servers. This example allows IT data center
servers to access DNS and NTP update servers and restricts communication to using only the necessary applications to establish connections to only the right set of update servers.

To create this rule:

1. Restrict the source of DNS and NTP update requests to only the data center servers that need to retrieve updates, in this example the DNS-NTP-Servers dynamic address group in the **Engineering-DC-Infra** zone.

2. Restrict the applications that data center servers can use to communicate with these external update servers to only the required applications, in this example, **dns** and **ntp**. Allow the applications to run only on the default port to prevent evasive malware from attempting to use non-standard ports.

3. Create a custom URL category to define the URLs of the update servers to which the data center servers can connect. In this example, the **NTP-DNS-Update-Servers** custom URL category defines the update server URLs that the data center servers can reach.

4. Apply the full suite of Security Profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.

5. Log update activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

**STEP 3** | Allow data center servers to access certificate authority servers to obtain the revocation status of digital certificates and ensure that they are valid.

This rule enables data center servers to connect to an Online Certificate Status Protocol (OCSP) Responder (server) on the internet to check the revocation status of authentication certificates. An OCSP Responder provides the most recent certificate status compared to browser Certificate Revocation List (CRL) updates, which depend on the frequency of CRL browser updates to keep up with certificate revocations, so the CRL is more likely to be out-of-date than an OCSP Responder. When you **configure a certificate profile** on the firewall, you can set up CRL status verification as a fallback method for OCSP in case the OCSP Responder is unreachable.

To create this rule:

1. Restrict the source of certificate revocation check requests to only the data center servers that need to check certificate validation, in this example the **IT-Server-Management** dynamic address group in the **IT-Infrastructure** zone.

2. Restrict the applications that data center servers can use to communicate with external certificate revocation servers to only the required applications. This example secures the connection between data center servers and OCSP Responders, so the only application to specify is **ocsp**. Allow the application to run only on the default port to prevent evasive malware from attempting to use non-standard ports.

3. Apply the full suite of Security Profiles to the rule to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.

4. Log activity so that you can track and analyze violations of the rule, which may indicate an attempted attack.

Verify that only the applications you explicitly whitelisted in the security policy rules are running by viewing the predefined Applications report (**Monitor > Reports > Application Reports > Applications**). If you see
unexpected applications in the report, review the application whitelist rules and refine them so that they
don't allow the unexpected applications.

Create Data-Center-to-Internet Decryption Policy Rules

Create Decryption policy rules to provide visibility into traffic from data center servers to the internet. Decrypt all traffic from data center servers to the internet. The only accounts initiating connections to the internet from inside the data center are service accounts and most of this traffic pertains to software updates, so there are no privacy issues to consider. It’s important to decrypt and inspect this traffic because if an update server is compromised, data center servers could download malware and propagate it through the software update process. Inspecting the traffic and applying the best practice threat prevention profiles protects your data center against malware that could otherwise be downloaded from a legitimate update server, using a legitimate application.

In Create Data-Center-to-Internet Application Whitelist Rules, we created Security policy rules that allow data center servers to initiate connections with internet update servers to update operating system software, DNS, NTP, and to check certificates. Here we create analogous Decryption policy rules to decrypt the traffic that the update Security policy rules allow.

*Do not decrypt traffic to certificate revocation servers (online responders). Online Certificate Status Protocol (OCSP) traffic usually uses HTTP, so the traffic is cleartext and not encrypted. In addition, SSL Forward Proxy Decryption may break the update process because the firewall acts as a man-in-the-middle proxy and replaces the client certificate with a proxy certificate, which the OCSP responder may not accept as valid.*

The decryption policy rules share some common elements in regard to these traffic flows:

- When you create a Decryption policy rule, the objective is to decrypt traffic so that a Security policy rule can examine it and allow or block it based on policy. To accomplish that, the Decryption policy rule must use the same source zone(s) and user(s) as the analogous security policy rule, and the same destination zone and address (often defined by a dynamic address group so that as you add or remove servers, you can update the firewall without a commit operation). Defining the same source and destination in the Security policy and in the Decryption policy applies both policies to the same traffic.
- The Action for all of these rules is decrypt.
- All of these decryption rules use the Best Practice data center decryption profile shown in Create the Data Center Best Practice Decryption Profiles.

In many cases, the Decryption policy rule examples include a custom URL category (Objects > Custom Objects > URL Category) to narrow the scope of traffic to decrypt. Each Decryption policy rule uses the same custom URL category (and source and destination) as the analogous Security policy rule so that the Decryption and Security policies apply to exactly the same traffic. The combination of App-ID and a custom URL category enables the firewall to decrypt only the traffic the whitelist rule allows, which saves processing cycles by not decrypting traffic that the firewall will block. (Decryption must happen before Security policy rule evaluation.)

**STEP 1 | Decrypt traffic between data center servers and software update servers on the internet.**

This rule shows how to decrypt data center server software update traffic to provide visibility into threats that may be present on internet update servers so the firewall can block them. This example decrypts allowed traffic between data center servers and CentOS update servers on the internet based on the analogous application whitelist rule we created earlier.
To create this rule:

- Specify the same source and destination as in the analogous Security policy rule. In this case, the source is the **Dev-Servers** dynamic address group in the **Engineering-DC-Infra** zone, and the destination is the internet (L3-External zone).
- Specify the same custom URL category as in the analogous Security policy rule (**CentOS-Update-Servers**) to narrow the scope of decryption to only traffic that the whitelist rule allows so that the firewall doesn’t waste cycles decrypting traffic that it will drop.
- On the Options tab, set the Action to **Decrypt** and the decryption Type to **SSL Forward Proxy**.

Apply the data center best practice Decryption Profile to apply SSL Forward Proxy and SSL Protocol Settings to the traffic.

Create a similar Decryption policy rule for the allowed data center traffic of each group of data center servers that needs to connect to internet update servers, based on the same source and destination, and same custom URL category, as the analogous Security policy rule. For example, the Decryption policy rule for data center servers that need to communicate with Microsoft Windows update servers, based on the analogous Security policy rule, looks like this:

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>URL Category</th>
<th>Action</th>
<th>Type</th>
<th>Decryption Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Update Decrypt</td>
<td>DC to Internet BP</td>
<td>Engineering-DC-Infra</td>
<td>Dev-Servers</td>
<td>L3-External</td>
<td>any</td>
<td>CentOS-Update-Servers</td>
<td>decrypt</td>
<td>SSL Forward Proxy</td>
<td>DC Best Practice</td>
</tr>
</tbody>
</table>

**STEP 2** Decrypt traffic between data center servers and NTP and DNS update servers on the internet.

This rule shows how to decrypt data center server NTP and DNS update traffic to provide visibility into threats that may be present on these internet servers so the firewall can block them. This example decrypts allowed traffic based on the analogous application whitelist rule we created earlier.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>URL Category</th>
<th>Action</th>
<th>Type</th>
<th>Decryption Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS-NTP Update Decrypt</td>
<td>DC to Internet BP</td>
<td>IT Infrastructure</td>
<td>DNS-NTP-Servers</td>
<td>L3-External</td>
<td>any</td>
<td>NTP-DNS-Update-Servers</td>
<td>decrypt</td>
<td>SSL Forward Proxy</td>
<td>DC Best Practice</td>
</tr>
</tbody>
</table>

To create this rule:

- Specify the same source and destination as in the analogous Security policy rule. In this case, the source is the **DNS-NTP-Servers** dynamic address group in the **IT Infrastructure** zone, and the destination is the internet (L3-External zone).
- Specify the same custom URL category as in the analogous Security policy rule (**NTP-DNS-Update-Servers**) to narrow the scope of decryption to only traffic that the whitelist rule allows.
- On the Options tab, set the Action to **Decrypt** and the decryption Type to **SSL Forward Proxy**.

Apply the data center best practice Decryption Profile to apply SSL Forward Proxy and SSL Protocol Settings to the traffic.
Define the Initial Intra-Data-Center Traffic Security Policy

Intra data center traffic flows between data center servers and application tiers. You could take the viewpoint that everything inside the data center perimeter is trusted so you don’t need to inspect that traffic. However, if an attacker compromises a data center server and the traffic between application tiers doesn’t go through firewalls, the attacker can move laterally through the data center to critical servers and download more malware, repurpose servers, and exfiltrate data using legitimate applications that have no place in the data center, as has happened in several major breaches over the past several years.

The best defense against malware that gains a foothold in the data center is to secure the traffic with strict, specific application whitelist rules and to inspect the traffic with next-generation firewalls placed between application tiers.

In addition, allow no unknown applications in the data center. Unknown applications may indicate that an adversary has gained access to your data center. Create custom applications for your proprietary internal applications so that you can identify them with App-ID and apply security to that traffic. If you don’t create custom applications for your proprietary applications, the firewall sees them as unknown-tcp or unknown-udp traffic. The issue is that the firewall treats the proprietary applications the same way it treats other unknown applications, and you should block unknown applications because they may be an attacker’s tools. If you allow unknown applications in your data center, you could be handing over the keys to your asset kingdom to an attacker.

For unknown commercial applications, you can submit a request to Palo Alto Networks to create an App-ID.

If you have existing Application Override policies that you created solely to define custom session timeouts for a set a of ports, convert the existing Application Override policies to application-based policies by configuring service-based session timeouts to maintain the custom timeout for each application and then migrating the rule the an application-based rule. Application Override policies are port-based. When you use Application Override policies to maintain custom session timeouts for a set of ports, you lose application visibility into those flows, so you neither know nor control which applications use the ports. Service-based session timeouts achieve custom timeouts while also maintaining application visibility.

- Intra-Data-Center Traffic Security Approach
- Create Intra-Data-Center Application Whitelist Rules
- Create Intra-Data-Center Decryption Policy Rules

Intra-Data-Center Traffic Security Approach

The traditional legacy approach to securing east-west traffic between data center servers leaves valuable assets exposed to risk, while the best practice approach protects your valuable assets.

<table>
<thead>
<tr>
<th>The Traditional Approach</th>
<th>Risk</th>
<th>The Best Practice Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>You don’t need to segment traffic that doesn’t cross the data center perimeter so traffic between application tiers doesn’t need to pass through the security infrastructure.</td>
<td>An attacker who compromises any data center server can move laterally to critical data center servers and repurpose them. Attackers inside the data center</td>
<td>Segment traffic between application tiers using tight whitelist rules to prevent unnecessary communication, reduce the attack surface, and help prevent an attacker from moving laterally within the data center</td>
</tr>
</tbody>
</table>
The Traditional Approach | Risk | The Best Practice Approach
--- | --- | ---
The data center is safe inside the trusted network, so it’s not urgent to patch data center servers quickly. | can move at will without fear of being discovered. | Install patches on data center servers in a timely manner to close down vulnerabilities. Creating whitelist security policy rules helps you understand what is running in your data center and where unpatched services are running.
Mix blocking and alerting threat prevention profiles from multiple vendors. | Vulnerabilities remain open longer and present attack vectors to attackers. | Install patches on data center servers in a timely manner to close down vulnerabilities. Creating whitelist security policy rules helps you understand what is running in your data center and where unpatched services are running.

In addition:
- Create a unique service account for each function. For example, allow only specific service accounts to replicate exchange mailboxes, and allow only specific service accounts on web servers to query MySQL databases. Don’t use one service account for both functions.
- Monitor service accounts.
- Don’t allow regular user accounts in the data center.

When you transition from port-based to application-based rules, in the rulebase, place the application-based rule above the port-based rule it will replace. Reset the policy rule hit counter for both rules. If traffic hits the port-based rule, its policy rule hit count increases. Tune the application-based rule until no traffic hits the port-based rule for a period of time, then remove the port-based rule.

### Create Intra-Data-Center Application Whitelist Rules

Data center traffic often consists of multi-tier application traffic that flows between different server tiers to provide services for applications such as SharePoint, WordPress, internal proprietary applications, etc. The most common multi-tier application architecture consists of web servers (presentation tier), application servers (application tier), and database servers (data tier). Create a Data Center Segmentation Strategy provides guidelines on how to place firewalls between application tiers and how to segment a data center.

The way you treat traffic between data center servers depends on the traffic. For most application traffic, add threat prevention profiles to the whitelist Security policy rules to inspect the traffic. For example, always apply the best practice Security Profiles to protect traffic between the web, application, and server tiers of finance applications, engineering development applications, and so on. The exception to applying threat prevention profiles is traffic for high-volume, low-value applications such as mailbox replication and backup flows. You still whitelist access to these applications, but because a firewall has already inspected the traffic before replication, applying threat prevention profiles consumes firewall CPU cycles without providing extra value.
The WildFire security profile identifies unknown malware attempting to spread among data center servers to prevent the exfiltration of data by discovering malware before it can do damage. If you can't use the WildFire global cloud, you can deploy a WildFire private cloud or a WildFire hybrid cloud.

The example Security policy rules in this section show how to whitelist traffic for multi-tier data center finance applications that require using the web server, application server, and database server tiers to serve the applications. The example includes two proprietary internal applications for which we created custom applications: Billing-App and Payment-App. Creating custom App-IDs for these applications enables the firewall to identify them, control them, and apply Security policy to them. Don't allow unknown applications in the data center because you can't identify and apply security to them, and they may indicate an adversary in your data center. Every data center application should have an App-ID.

Allow applications only on their standard (application-default) ports. In some cases, business needs may require you to make an exception and allow applications to use non-standard ports between particular clients and servers. In these cases, be aware of the application traffic running on non-standard ports, and ensure that you know every instance of an application running on a non-standard port. Applications that run on non-standard ports for which you have not made an explicit (known) exception may indicate the presence of evasive malware.

Tag all sanctioned applications with the predefined Sanctioned tag. Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.

Order the Data Center Security Policy Rulebase shows you how to order these rules with all of the other rules we create for the other three data center traffic flows and the block rules so that no rule shadows another rule.

To apply consistent security policy across multiple data centers, you can reuse templates and template stacks so that the same policies apply to every data center. The templates use variables to apply device-specific values such as IP addresses, FQDNs, etc., while maintaining a global security policy and reducing the number of templates and template stacks you need to manage.

STEP 1 | Allow finance application traffic between the web server tier and the application server tier.

This rule restricts the traffic that can flow between the web server tier and the application server tier for the Finance department's billing servers so that only traffic using legitimate applications can access the billing servers. (We also create a rule to restrict Finance user access to the data center when we Create User-to-Data-Center Application Whitelist Rules so that only the right Finance users can access the data center.) The rule uses dynamic address groups to specify the servers in each application tier—Web-Servers specifies the addresses of the servers in the web server tier and Billing-App-Servers specifies the addresses of the servers in Finance's billing application server tier.

To create this rule:

- Restrict the source of finance application traffic to the web servers (Web-Servers) in the Web-Server-Tier-DC zone.
• Restrict the destination for finance application traffic to the billing servers (Billing-App-Servers) in the App-Server-Tier-DC zone.

• Restrict the applications the web servers can use to access the billing application servers and only allow applications on their default ports. In this example, the applications include two custom applications, Billing-App and Payment-App, for which you specify default ports when you create the applications. The Finance Department uses these proprietary applications for billing and payment services.

• Apply the full suite of best practice security profiles to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.

• Log activity so that you can track and analyze rule violations, which may indicate an attempted attack.

Create similar rules to control applications and traffic between the web server tier and other application server tiers.

**STEP 2 | Allow finance application traffic between the applications server tier and the database server tier.**

This rule restricts the traffic that can flow between the application server tier and the database server tier for the Finance department's billing servers so that only traffic using legitimate applications can flow between the billing application servers and the billing database servers. The rule uses dynamic address groups to specify the servers in each application tier—Billing-App-Servers specifies the addresses of the servers in the application server tier and DB2-Servers specifies the addresses of the servers in Finance's database server tier.

To create this rule:

• Restrict the source of finance application traffic to the billing application servers (Billing-App-Servers) in the App-Server-Tier-DC zone.

• Restrict the destination for finance application traffic to the database servers (DB2-Servers) in the DB-Server-Tier-DC zone.

• Restrict the applications the billing application servers can use to access the database servers and only allow applications on their default ports or their known non-default ports.

• Apply the full suite of best practice security profiles to protect against malware, vulnerabilities, C2 traffic, and known and unknown threats.

• Log activity so that you can track and analyze rule violations, which may indicate an attempted attack.

Create similar rules to control applications and traffic between the application server tier and database server tier for other applications.

Verify that only the applications you explicitly whitelisted in the security policy rules are running by viewing the predefined Applications report (Monitor > Reports > Application Reports > Applications). If you see unexpected applications in the report, review the application whitelist rules and refine them so that they don't allow the unexpected applications.
Create Intra-Data-Center Decryption Policy Rules

Why decrypt traffic inside the data center? After all, there are no users and the data center is a safe environment deep inside the secure network. But nothing could be farther from the truth. The data center is a perfect place for attackers to hide precisely because many people think the data center is safe and don’t look there. But the same basic tenet that’s true in the rest of the network holds true in the data center: you can’t protect yourself against what you can’t see. Decrypt encrypted data center traffic so that the firewall can inspect traffic, control access, make threats visible, and protect your valuable assets.

Some data center traffic is unencrypted (cleartext). Don’t enable decryption on cleartext flows because there is nothing to decrypt.

In Create Intra-Data-Center Application Whitelist Rules, we created Security policy rules that allow servers involved with Finance Department applications that are in different application tiers to communicate with each other. Here we create analogous Decryption policy rules to decrypt the traffic that those rules allow.

STEP 1 | Decrypt finance application traffic between the web server tier and the application server tier.

This rule decrypts the traffic flowing between the web server tier and the application server tier for the Finance department’s billing servers so that the firewall can see the traffic and protect the servers in each tier against potential threats.

To create this rule:

- Specify the same source and destination as in the analogous Security policy rule. In this example, the source is the Web-Servers dynamic address group in the Web-Server-Tier-DC zone, and the destination is the Billing-App-Servers in the App-Server-Tier-DC zone.
- On the Options tab, set the Action to Decrypt and the decryption Type to SSL Forward Proxy. Apply the data center best practice Decryption Profile to apply SSL Forward Proxy and SSL Protocol Settings to the traffic.

STEP 2 | Decrypt finance application traffic between the application server tier and the database server tier.

This rule decrypts the traffic flowing between the application server tier and the database server tier for the Finance department’s billing servers so that the firewall can see the traffic and protect the servers in each tier against potential threats.

To create this rule:

- Specify the same source and destination as in the analogous Security policy rule. In this example, the source is the Billing-App-Servers dynamic address group in the App-Server-Tier-DC zone, and the destination is the DB2-Servers in the DB-Server-Tier-DC zone.
- On the Options tab, set the Action to Decrypt and the decryption Type to SSL Forward Proxy. Apply the data center best practice Decryption Profile to apply SSL Forward Proxy and SSL Protocol Settings to the traffic.
Order the Data Center Security Policy Rulebase

This section summarizes the data center Security policy rulebase for all four data center traffic flows to provide a snapshot of the complete rulebase and show the order of the rules. The preceding sections discuss each Security policy rule in detail (as well as the Decryption policy rules, and where required, the Authentication policy and DoS Protection policy rules).

The order of the rules is critical. No rule should shadow another rule. For example, block rules should not block traffic that you want to allow, so a whitelist rule must allow traffic that a block rule blocks before the block rule goes into effect. In addition, a whitelist rule should not allow traffic that you want to block. By creating very specific whitelist rules, you can tightly control the allowed applications and who can use them, and then block those applications from other users who are not sanctioned to use them.

The first five rules whitelist DNS access for users and whitelist specific application and server access for specific user groups. These are the rules we configured in Create User-to-Data-Center Application Whitelist Rules.

Only the specified users can use only the specified applications on their default ports to access only the specified data center destination servers (addresses). Security profiles protect all of these allow rules against threats. These rules precede the block rules that discover unknown users and applications on the network because these rules are very specific and prevent sanctioned users and applications from matching more general rules lower in the rulebase.

The next two block rules, which we created in Create Data Center Traffic Block Rules, discover unexpected applications from users on standard ports and on non-standard ports.

The preceding whitelist rules allow access for known users, running only the applications they need to use for business purposes on standard (application-default) ports. Traffic from known users running the same applications on non-standard ports doesn’t match those whitelist rules and filters through to the following known-user rule, which logs the non-standard port usage and applies threat protection profiles to the traffic.
Because these rules are based on traffic from the user zones, traffic from other zones doesn’t match these rules. Place these rules above the application blocking rules (rules 16 and 17) or they will shadow these rules. (Traffic that matches these two rules may also match the more general application blocking rules. If the application blocking rules come first and match traffic that also matches these rules, that traffic won’t hit these rules and won’t be logged separately, so the rules won’t do their intended job of differentiating blocking that is the result of employee user activity from blocking that is the result of activity from other zones.)

The next seven rules whitelist traffic for the rules we created in Create Internet-to-Data-Center Application Whitelist Rules, Create Data-Center-to-Internet Application Whitelist Rules, and Create Intra-Data-Center Application Whitelist Rules.

Security profiles protect all of these allow rules against threats.

The next four rules, which we configured in Create Data Center Traffic Block Rules, block applications that you know you don’t want in your data center and unexpected applications, and discover unknown users on your network.
Rule 15 blacklists applications you never want in your data center. This rule comes after the whitelist allow rules to allow exceptions. For example, you may sanction one or two file sharing applications in application whitelist rules that precede this blacklist rule, and then the application filter in this rule blocks the rest of that application type to prevent the use of unsanctioned file sharing applications. If there are sets of applications or individual applications that you never want on your network and for which there are no exceptions, for example, BitTorrent, you can create a specific blacklist rule to block just those applications and place it at the top of the rulebase, above the application whitelist rules. However, if you do this, you must be certain that none of the blacklisted applications have legitimate business uses because they will be blocked.

Rules 16 and 17 are analogous to rules 6 and 7, which discover unexpected applications from users (the traffic those rules apply to comes only from user zones). Rules 16 and 17 discover unexpected applications from all other zones. Having separate rules enables you to log blocking rule matches with greater granularity.

Rule 18 discovers unknown users so that you can log those attempted accesses separately for easier investigation.

As with all Security Policy rulebases, the final two rules are the standard Palo Alto Networks default rules for intrazone traffic (allow) and interzone traffic (deny).
Log and Monitor Data Center Traffic

The firewall’s logging and monitoring tools reveal applications, users, and traffic patterns on your network, including applications and users you may not have known were there. Logging and monitoring provides useful information at all stages of the transition to and maintenance of a data center best practice security policy because it also reveals unknown users (not identified by User-ID), unknown applications, and traffic on unexpected ports, all of which indicate that a Security policy rule has not be correctly or tightly constructed. Logging and monitoring information help you determine which applications to allow and which users to allow access to which applications and devices, and also helps you investigate potential security issues.

When you assess your data center, you capture baseline measurements. Periodically compare those baseline measurements with current measurements to evaluate progress, identify changes, and find areas for improvement as you implement your data center best practice Security policy.

If you use Panorama to manage firewalls, you can monitor firewall health to compare devices to their baseline performance and to each other to identify deviations from normal behavior.

Configure log forwarding from firewalls to Panorama or to external services such as an SNMP Trap server or a syslog server to centralize the logs from multiple firewalls for more convenient viewing and analysis (a firewall can only display local logs and reports, not logs and reports from other firewalls). When you configure log forwarding, configure sending notifications to verify that the log destinations you configure are receiving the firewall logs.

Best practices for data center logging and monitoring include:

- What Data Center Traffic to Log and Monitor
- Monitor Data Center Block Rules and Tune the Rulebase
- Log Data Center Traffic That Matches No Interzone Rules
- Log Intra Data Center Traffic That Matches the Intrazone Allow Rule

What Data Center Traffic to Log and Monitor

The Palo Alto Networks next-generation firewall creates some logs by default, while you need to configure logging for other traffic. The best practice is to log all data center traffic and monitor the logs for unexpected applications, users, traffic, and behaviors.

By default, the firewall logs traffic that matches explicitly configured Security policy rules and does not log traffic that matches the predefined intrazone-default (allows traffic with a source and destination in the same zone) and interzone-default (the last rule in the rulebase, which denies traffic that matches no preceding rules) rules at the bottom of the rulebase.

When you create a Security policy rule and the firewall logs its traffic by default, the firewall logs the traffic at the end of the session:
The best practice for most traffic is to **Log at Session End** because applications often change throughout the lifespan of a session. For example, the initial App-ID for a session may be web-browsing, but after the firewall processes a few packets, the firewall may find a more specific App-ID for the application and change the App-ID. There are several use cases for logging traffic at the start of a session, including DNS sinkholing, long-lived tunnel sessions, and when you need information from the start of the session for troubleshooting.

Logging the traffic records information about traffic that a rule allows and traffic that a rule denies or drops (rule violations), so the firewall provides valuable information regardless of how the it treats the traffic. Rule violations highlight potential attacks or whitelist rules that need to be adjusted to allow a legitimate business application.

When you examine blocked traffic in logs, differentiate between traffic that the firewall blocked as a protective event before any systems have been compromised, such as blocking an application that isn’t whitelisted, and traffic that the firewall blocked as a post-compromise event, for example, an attempt by malware that is already on a data center server to contact an external server to download more malware or exfiltrate data.

The firewall provides a wealth of monitoring tools, logs, and log reports with which to analyze your network:

- **Monitor > Logs** provides traffic, threat, User-ID, and many other log types, including Unified logs, which show multiple log types on one screen so you don’t have to look at different types of logs separately. When a magnifying glass icon is part of the summary, you can click it to drill down into the log entry.
- **Monitor > PDF Reports** provides predefined reports that you can view and the ability to create report groups composed of predefined and custom reports. For example, you can review traffic activity or take baseline measurements to understand the bandwidth usage and traffic flow in each data center segment by zone or interface.
- **Monitor > Manage Custom Reports** provides the ability to create customized reports so that you can view information about block rules, allow rules, or any other subject of interest.
- **Monitor > Packet Capture** enables you to take packet captures of traffic that traverses the firewall’s management interface and network interfaces.
- The Application Command Center (ACC) provides widgets that display an interactive, graphical summary of the applications, users, URLs, threats, and content traversing the network. For example, you can review and evaluate the applications on the network (ACC > Network Activity > Application Usage > Threats) to see if there are any changes in the application or if the application exhibits threat behaviors. If you see unexpected applications in the list, evaluate how to handle those applications.

Another good way to use ACC information is to help identify compromised user accounts and host systems. Analyze threats along with the usernames associated with the threats using the ACC >
Network Activity > User Activity > Threats widget and then use the threat logs to isolate the exact issue.

- The Dashboard (Dashboard) provides widgets that display general firewall information and up to 10 of the most recent entries in the threat, configuration, and system logs.
- Use Panorama to monitor firewall health and baseline new devices, to compare performance metrics, and to track firewall performance after an event such as a commit, a software upgrade, content updates, rule changes, the addition of new applications, etc. If performance deviates from a device’s baseline, you can view and troubleshoot manually or automatically open a ticket for investigation.
- On Panorama or on an individual firewall, use the policy rule hit counter to analyze changes to the rulebase. For example, when you add a new application, before you allow that application’s traffic on the network, add the allow rule to the rulebase. If traffic hits the rule and increments the counter, it indicates traffic that matches the rule may already be on the network even though you haven’t activated the application, or that you need to tune the rule. Another example is replacing port-based rules with application-based rules by placing the application-based rule before the port-based rule and noting if any traffic hits the port-based rule. If traffic hits the port-based rule, then you need to tune the application-based rule to catch that traffic.

In conjunction with the policy rule hit counter, check the ACC > Threat Activity > Applications Using Non Standard Ports and the ACC > Threat Activity > Rules Allowing Apps On Non Standard Ports widgets to see if traffic on non-standard ports caused the unexpected rule hits.

The key to using the policy rule hit counter is to reset the counter when you make a change, such as introducing a new application or changing a rule’s meaning. Resetting the hit counter ensures that you see the result of the change, not results that include the change and events that happened before the change.

Monitor Data Center Block Rules and Tune the Rulebase

Developing a best practice security policy is an iterative process. As soon as you Create Data Center Traffic Block Rules, start monitoring traffic that matches the block rules designed to identify policy gaps, unexpected behaviors, and potential attacks. Tune your application whitelist rules to account for traffic that matches the block rules but should be allowed and investigate traffic that may indicate an attack.

Reports on blocked traffic contain valuable information you can use to investigate potential issues. Keep the block rules in the rulebase to protect your valuable data center assets and provide that information when traffic matches a block rule.

Follow content update best practices to keep your firewall protection up-to-date. Maintain the Data Center Best Practice Rulebase includes specific best practices for data center firewalls.

STEP 1 | Create custom reports to monitor traffic that matches the block rules designed to identify policy gaps and potential attacks.

1. Select Monitor > Manage Custom Reports.
2. Add a report and give it a Name that describes the report’s purpose, in this example DC Best Practice Policy Tuning.
3. Set the Database to Traffic Summary. (This also changes the default Selected Columns; the default columns are Source Zone, Destination Zone, Sessions, and Bytes.)
4. Select the Scheduled box.
5. From Available Columns, add Application, Risk of App, Rule, and Threat to the Selected Columns list. If there are other types of information you want to monitor, select those as well.
6. Set the desired Time Frame, Sort By, and Group By values, in this example Last 7 Days, Apps, and App Sub Category, respectively.
7. Define the query to match traffic hitting the rules designed to find policy gaps and potential attacks. You can create a single report for traffic that matches any of the rules using the **or** operator, or create individual reports to monitor each rule. In the **Query Builder**, specify the name of each rule you want to include in the report. This example uses the names of the six blocking rules designed to find policy gaps and uses the **Or** operator to include information about traffic that matches any of the rules:

- (rule eq 'Known user nonstandard ports')
- (rule eq 'Unknown user nonstandard ports')
- (rule eq 'Unexpected App from user Zone')
- (rule eq 'Unexpected App from any Zone')
- (rule eq 'Unexpected User App Any Port')
- (rule eq 'Unexpected App Any Port')

**STEP 2 |** Review the report (or reports) regularly to make sure you understand why traffic matches each block rule and either update policy to include legitimate applications and users, or use the information to assess the risk of traffic that matches the rules.

**Log Intra Data Center Traffic That Matches the Intrazone Allow Rule**

By default, all intrazone traffic (source and destination in the same zone) is allowed. After the firewall evaluates Security policy, it either allows traffic controlled by application whitelist rules, denies traffic controlled by block rules, or if intrazone traffic matches no rules, the firewall allows it by default. (The firewall blocks interzone traffic by default.) Because of the valuable nature of data center assets, the best practice is to monitor all traffic inside the data center between data center servers, including traffic allowed by the intrazone default allow rule.
To gain visibility into this traffic, enable logging on the intrazone-default rule when it applies to traffic within zones inside the data center. Logging this traffic gives you the opportunity to examine access that you have not explicitly allowed and which you may want to either explicitly allow by modifying a whitelist rule or explicitly block.

In Define the Initial Intra-Data-Center Traffic Security Policy, we used three example zones inside the data center: Web-Server-Tier-DC, App-Server-Tier-DC, and DB-Server-Tier-DC. In this example, we create a custom report to gather log information about data center intrazone traffic in these three internal data center zones.

**STEP 1** | Select the intrazone-default row in the rulebase and click Override to enable editing the rule.

**STEP 2** | Select the intrazone-default rule name to edit the rule.

**STEP 3** | On the Actions tab, select Log at Session End and click OK.

**STEP 4** | Create a custom report to monitor traffic that hits this rule for the internal data center zones.

1. Select Monitor > Manage Custom Reports.
2. Add a report and give it a descriptive Name. In this example, the name is Log Intrazone-Default Rule-DC.
3. Set the Database to Traffic Summary.
4. Select the Scheduled box.
5. From Available Columns, add Application, Risk of App, Rule, and Threat to the Selected Columns list. If there are other types of information you want to monitor, select those as well.
6. Set the desired Time Frame, Sort By, and Group By values. In this example, the selected values are Threats and App Category, respectively.
7. Define the query to match traffic that matches the intrazone-default rule for the data center zones:

   (rule eq interzone-default) and ((zone eq Web-Server-Tier-DC) or (zone eq App-Server-Tier-DC) or (zone eq DB-Server-Tier-DC))

The query filters for traffic that matches the interzone default rule and also matches any of the three internal data center zones that we defined. Because the default Selected Columns include zones, the report shows the zone for each session. In a real-world data center, you would probably have more zones and you would add each zone to the query. The resulting custom report settings look like this:
8. **Commit** the changes.

**Log Data Center Traffic That Matches No Interzone Rules**

Traffic that doesn’t match any of the Security policy rules you configure matches the predefined interzone-default rule at the bottom of the rulebase and is denied. To gain visibility into traffic that doesn’t match a rule you explicitly configured, enable logging on the interzone-default rule. Logging this traffic gives you the opportunity to examine access attempts that you have not explicitly allowed, which may identify attack attempts or traffic for which you want to modify a whitelist rule to allow.

**STEP 1** | Select the interzone-default row in the rulebase and click **Override** to enable editing the rule.

**STEP 2** | Select the **interzone-default** rule name to edit the rule.

**STEP 3** | On the Actions tab, select **Log at Session End** and click **OK**.

**STEP 4** | Create a **custom report** to monitor traffic that hits this rule.

1. Select **Monitor > Manage Custom Reports**.
2. **Add** a report and give it a descriptive **Name**. In this example, the name is **Log Interzone-Default Rule**.
3. Set the **Database** to **Traffic Summary**.
4. Select the **Scheduled** box.
5. From **Available Columns**, add **Application**, **Risk of App**, **Rule**, and **Threat** to the **Selected Columns** list. If there are other types of information you want to monitor, select those as well.
6. Set the desired **Time Frame**, **Sort By**, and **Group By** values. In this example, the selected values are **Threats** and **App Category**, respectively.
7. Define the query to match traffic that matches the interzone-default rule:
(rule eq interzone-default)

The resulting custom report settings look like this:

8. Commit the changes.
Maintain the Data Center Best Practice Rulebase

Applications constantly evolve, so your application whitelist needs to evolve with them. Because the best practice rules leverage policy objects to simplify administration, adding support for a new application or removing an application from your whitelist typically means modifying the corresponding application group or application filter accordingly.

Palo Alto Networks sends content updates that you should download automatically and schedule for installation on firewalls as soon as possible. Most content updates contain updates to threat content (antivirus, vulnerabilities, anti-spyware, etc.) and may contain modified App-IDs. On the third Tuesday of each month, the content update also contains new App-IDs. You can set separate thresholds to delay installing regular content updates and to delay installing the once-a-month update that contains new App-IDs for a specified period of time after the download. Delaying installation enables you to install content updates that don’t include new App-IDs as quickly as possible to get the latest threat signatures, while also providing more time to examine new App-IDs before installing them.

The content updates on the third Tuesday of each month that contain new App-IDs may cause changes in Security policy enforcement. Before you install new or modified App-IDs, review the policy impact, stage updates to test impact, and modify existing Security policy rules if necessary. The most efficient way to control downloading and installing content updates on firewalls is loading them on and pushing them from Panorama if you use Panorama.

Follow the general content update best practices, but keep in mind that data center availability is usually critical, so you may not choose to roll out content updates as fast in the data center as you would on internet-facing firewalls:

- Quickly test content updates in a safe area of the network before you install them in the data center.
- For content updates that don’t contain new App-IDs, set the installation threshold to no more than eight hours after the automatic download and conduct testing within that period.
- For content updates that contain new App-IDs, set the installation threshold to no more than eight days after the automatic download and conduct testing within that period.
- Configure Log Forwarding for all content updates.

**STEP 1 |** Before installing a new content update, review new and modified App-IDs to determine if there is policy impact.

**STEP 2 |** If necessary, modify existing Security policy rules to accommodate the App-ID changes.

You can disable selected App-IDs if some App-IDs require more testing and install the rest of the new App-IDs. Finish testing any necessary policy revisions before the next monthly content release with the new App-IDs arrives (third Tuesday of each month) to avoid overlap.

Over time, the list of applications used in the data center usually stabilizes, so fewer and fewer new App-IDs are relevant. (Most new App-IDs pertain to internet-facing applications.) This reduces the risk of new App-IDs creating an issue in the data center and may enable you to install content updates with new App-IDs faster.

**STEP 3 |** Prepare policy updates to account for App-ID changes included in a content release or to add new sanctioned applications to or remove applications from your whitelist rules.

Other ways to maintain the best practice rulebase include:

---

*DATA CENTER BEST PRACTICE SECURITY POLICY | Data Center Best Practice Security Policy*  
© 2019 Palo Alto Networks, Inc.
• Use Palo Alto Networks Assessment and Review Tools to identify gaps in security coverage.
• User feedback about applications they can no longer access may identify gaps in the rulebase or risky applications that were in use on your network before positive enforcement prevented their use.
• Compare the asset inventory list you created when you assessed your data center to the assets themselves and ensure that those assets are protected appropriately.
• Use Palo Alto Networks logging and monitoring tools such as the Application Command Center (ACC) to find and investigate unexpected activity, which may indicate a misconfigured or missing rule. Run reports periodically to check that the level of security you want to apply is applied.

If you use Panorama to manage firewalls, you can monitor firewall health to compare devices to their baseline performance and to each other to identify deviations from normal behavior.
Use Palo Alto Networks Assessment and Review Tools

The Customer Success Team at Palo Alto Networks has developed a prevention architecture with tools and resources to help you review and assess the security risks of your network and how well you have used the capabilities of the firewall and other tools to secure your network. Contact your Palo Alto Networks representative to schedule assessments and reviews (a Palo Alto Networks sales engineer conducts the reviews to provide expertise in assessing the security state of your network). As of this publication, the available Security Risk prevention tools include:

- **Prevention Posture Assessment (PPA)**—The PPA is a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture. The PPA not only helps to identify all security risks, it also provides detailed suggestions on how to prevent the risks and close the gaps. The assessment, guided by an experienced Palo Alto Networks sales engineer, helps determine the areas of greatest risk where you should focus prevention activities. You can run the PPA on firewalls and on Panorama.

- **Best Practice Assessment (BPA) Tool**—The BPA for next-generation firewalls and Panorama evaluates a device’s configuration by measuring the adoption of capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks.

  The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories. The results include trending data, which shows the rate of security improvement as you adopt new capabilities, fix gaps, and progress toward a Zero-Trust network.

  The BPA component performs more than 200 security checks on a firewall or Panorama configuration and provides a pass/fail score for each check. Each check is a best practice identified by Palo Alto Networks security experts. If a check returns a failing score, the tool provides the justification for the failing score and how to fix the issue.

Palo Alto Networks continues to develop new tools and refine existing tools. Contact your Palo Alto Networks representative to find out what the most current tools can do to increase your data center network security.