

CONTENT SECURITY

.....

Corporate intranet protection is a major concern among most businesses connected to the Internet. These concerns range from virus activity, to employees surfing points unknown on the Web. Check Point content security, provided through VPN-1 NGX resources, helps alleviate these concerns.

NGX content-security features allows Administrators to do the following:

- Distribute content security to multiple Security Gateways.
- Screen URLs, and block suspicious Web data.
- Provide auditing capabilities and detailed reports.

Objectives

Distribute content security to Security Gateways, screen URLs and block suspicious Web data, and provide auditing capabilities and detailed reports:

1. Configure content security to meet business requirements.
2. Configure resource objects to support auditing capabilities and detailed reports.
3. Identify and correct problems with resource objects and rules, given symptoms of a configuration problem.

▪
▪
▪
▪
▪

Key Terms

- Content Vectoring Protocol (CVP)
- Anti-virus inspection
- URI Filtering Protocol (UFP)
- Common Internet File System (CIFS)
- Security Server

ROLE OF THE SECURITY SERVER

When a new connection is initiated, the Security Gateway determines whether or not to allow the connection into a protected network. If the Rule Base includes a rule with a resource in the Service column or if User Authentication is specified in the Action column, the Security Server for the specified service is invoked.

Security Servers broker connections between clients and servers. Addresses and ports are translated, so to both participants, it appears the connection is direct. However, an observation of the traffic reveals the Security Server's role.

The following is a list of NGX Security Servers:

- Telnet
- rlogin
- FTP
- HTTP
- SMTP

Security Server Overview

Security Servers perform two tasks: authentication and content security. The following table shows the functions each NGX Security Server performs:

Server	Authentication	Content Security
Telnet	Yes	No
rlogin	Yes	No
FTP	Yes	Yes
HTTP	Yes	Yes
SMTP	No	Yes



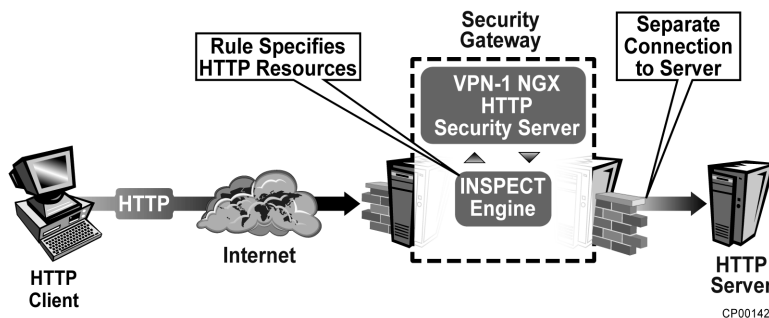
See the OPSEC Solutions Center at www.opsec.com for a complete list of OPSEC certified products and their compatibility with NGX product releases:



Only OPSEC certified products are supported by Check Point Software.

UNDERSTANDING CONTENT SECURITY

Content security extends the scope of data inspection to the highest level of a service's protocol, achieving highly tuned access control to network resources. An NGX resource specification defines a set of entities that can be accessed by a specific protocol. You can define a resource, based on HTTP, FTP, SMTP, CIFS, or a generic TCP resource. For example, you might define a URI resource whose attributes are a list of URLs, and HTTP and FTP schemes. The resource can be used in a Rule Base the same way a service can, with standard logging and alerting methods available for monitoring.



A Connection Mediated by an HTTP Security Server

For each connection that is established through an NGX Security Server, the Administrator is able to control specific access according to fields that belong to the specific service. When a resource is specified, the Security Server can divert the connection to a Content Vectoring Protocol (CVP) or URI Filtering Protocol (UFP) server.

When a rule specifies a resource in the service field of a Rule Base, the NGX Gateway diverts all packets in the connection to the corresponding Security Server, which performs the required content-security inspection. If the connection is allowed, the Server opens a second connection to the final destination.

For each connection established through an NGX Security Server, the Administrator is able to control specific access, according to fields that belong to the specific service: URLs, filenames, FTP **PUT** and **GET** commands, types of requests, and others. Major security enhancements enabled by the content-security feature are CVP checking for files transferred and URI filtering.



When a resource is specified, the Security Server can divert the connection to one of the following servers:

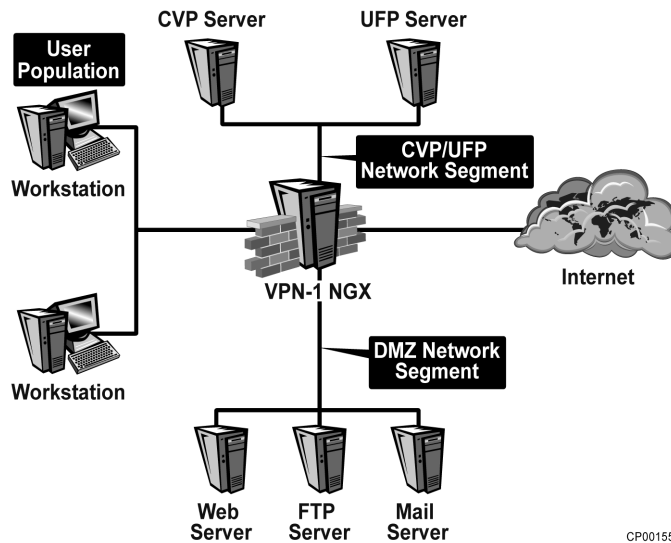
Content Vectoring Protocol (CVP) — Examines and reports on the contents of files, for example, whether a file contains a virus; a CVP server can also examine the content of outgoing data packets, before establishing an outgoing connection to an HTTP Web server.

URI Filtering Protocol (UFP) — Maintains a list of URLs and their categories

The URI Filtering Protocol is used to protect against specific destinations on the Internet. This Security Server can determine user rights, including the ability to visit a particular Web site or download certain file types. This capability is integrated into VPN-1 NGX, and does not require additional software. There are some limits, however, and the integrated capabilities do not scale to cover large numbers of restricted sites. This should be used primarily for restricting less than 50 URLs to the user population. This limitation is not a hard limit, but is more of a practical maintenance issue. These entries into the Security Server are manually performed, thus making it somewhat difficult to have as many banned sites as some OPSEC partners' solutions allow.

CONTENT VECTORING PROTOCOL (CVP)

There is no virus-scanning capability integrated into VPN-1 NGX. The Security Server is in place to allow the NGX Gateway to transfer packets to another server running an OPSEC certified virus scanner. This method uses CVP to transfer packets to and from an OPSEC virus-scanning server.



CP00155

CVP Server Integration

By default, CVP uses TCP port 18181, and is designed to reroute data streams to an external virus-scanning server. The virus scanner determines if there is a virus, and returns the file to the NGX Gateway, if it is virus-free. Using CVP Security Servers for virus scanning assists network security in several ways:

- Eliminates viruses from being downloaded from FTP or HTTP transfers
- Prevents malicious-script viruses from entering through e-mail
- Off-loads the scanning process to another machine away from the NGX Gateway, improving performance of the Gateway

These servers are typically either placed in the DMZ, or on a private-network segment with a Gateway. This allows fast, secure connections between the CVP servers and the Gateway.

When a resource specifies a CVP server, VPN-1 NGX passes the file to a virus-scanning server for inspection. This occurs, if an Administrator specified that a file undergo a virus check, before allowing it to be sent to the client.

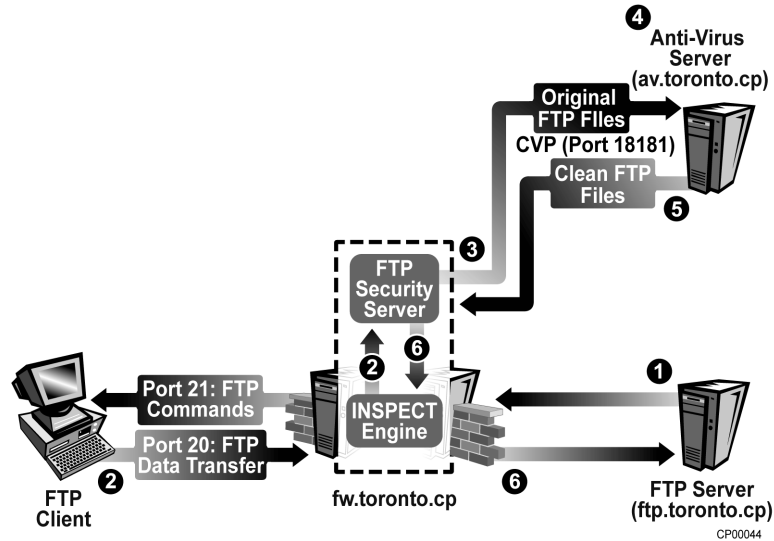


For a list of OPSEC compliant virus-scanning servers, see www.opsec.com.

Inspection

Anti-virus inspection reduces the vulnerability of hosts and gateways. With the use of an external Anti-Virus Module or CVP server, the anti-virus option can check all files transferred for HTTP, FTP, SMTP, and other TCP protocols.

This figure illustrates how VPN-1 NGX implements CVP for virus checking in an FTP connection:



FTP to Anti-Virus-Server Process

1. The FTP client establishes a connection via port 21 to the FTP server. The Gateway monitors port 21 for GET and PUT commands.
2. When the client initiates a data transfer over port 20, the Gateway folds the connection into the FTP Security Server.
3. The FTP data stream is relayed to the anti-virus server.
4. The CVP server scans FTP files. The results of the scan are sent to the Gateway.
5. The clean FTP file is resent to the FTP Security Server via CVP.
6. The FTP Security Server determines whether the GET or PUT command is allowed, and relays the FTP file to ftp.toronto.cp.



URI FILTERING PROTOCOL (UFP)

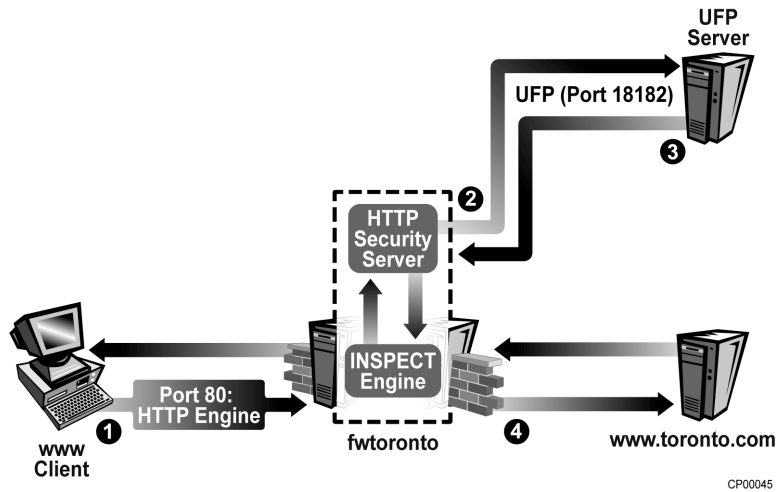
URI Filtering Protocol (UFP) is a Check Point developed application-programming interface (API). UFP enables the integration of third-party applications, to categorize and control access to specific URL addresses through the OPSEC security-management framework.



For a list of OPSEC compliant URL screening servers, see www.opsec.com.

A UFP server is used to specify a list of URLs. A UFP server has a predefined list of categories that can be downloaded. You can select individual categories, from the list in the definition of the resource that use this UFP server.

UFP uses TCP port 18182, and scans for and forwards detected URLs to a UFP server.



Simple UFP-to-Content-Server Process

- *URI Filtering Protocol (UFP)*
-
-
-
-

How UFP Works

VPN-1 NGX implements UFP by following these steps:

1. A client invokes a connection through a Gateway.
2. An NGX Security Server uses UFP to send the third-party UFP server the URL to be categorized.
3. A URL Content Server inspects the file and returns a validation-result message, notifying the Security Server of the result of the inspection.
4. The Gateway takes the action defined for the resource, either allowing or disallowing the viewing of that particular Web page.



IMPLEMENTING CONTENT SECURITY

To implement content security, follow these steps:

1. Create an object for the third-party server.
2. Create a UFP/CVP OPSEC application object for the third-party server.
3. Define a resource that specifies matching, and the type of content-checking action.
4. Define rules that specify an action taken for the resource.

There are two different methods for implementing Security Servers: active implementation requiring user interaction, and passive implementation where everything is transparent to users. Consideration must be given to the knowledge level and ability of end users, when determining whether to use active or passive Security Servers.

The active method can improve security, by requiring users to authenticate in order to use a specific service. This allows a time-out on passwords, and users must reauthenticate at a specified time period.

The passive method is transparent to end users. This prevents additional passwords from being used, and will probably result in fewer complaints. This method also requires the least amount of training, since the only way an end user knows about the Security Server, is if it prevents him from visiting a site that is on the banned list. In most cases, this is not reported as a problem.

CVP servers are transparent to end users. There should not be a need for user interaction, when using anti-virus or other CVP software on a Gateway.

Security Considerations

As an Administrator, you may desire a combination of the two methods. This allows the most flexibility for various environments. The active method can be used for a majority of users, or where there is a significant concentration of people. This will prevent unauthorized users from using other machines to access information through a Gateway. Other users in more restrictive physical environments, or who are constantly passing traffic through a Gateway, may be configured to use a transparent-authentication scheme.

▪
▪
▪
▪
▪

Virus scanning at the Gateway level is a good practice. But it is recommended that desktop anti-virus software be used, as well. This provides overlapping layers of defense in the network.

URI Filtering

URI filtering provides precise control over Web access, allowing Administrators to define undesirable or inappropriate Web pages. VPN-1 NGX checks Web connection attempts using UFP servers. UFP servers maintain lists of URLs and their appropriate categories — permitted or denied. URI databases can be updated to provide a current list of blocked sites. All communication between VPN-1 NGX and the URI filtering servers is in accordance with the UFP.

To implement URI filtering:

1. Define a UFP server: UFP servers are defined in the UFP Group Properties screen.
2. Define a URI resource that specifies a list of URL categories from the UFP server. The URI resource is defined in the URI Definition screen — UFP Specification. The URI resource specifies the UFP server, and a list of URL categories provided by the server.
3. Define rules that specify an action taken for the resource. For example:

Allowed — HTTP and FTP schemes, **GET** and **POST** methods

Not Allowed — A list of forbidden URL categories

4. Specify whether CVP is to be implemented. CVP fields are defined in the CVP tab of the URI Definition screen. The Administrator must define whether or not CVP is to be used. The Administrator must then select the CVP server. The Administrator defines whether or not the CVP server is allowed to modify content, and whether or not to send HTTP headers to the CVP server.

Mail — SMTP

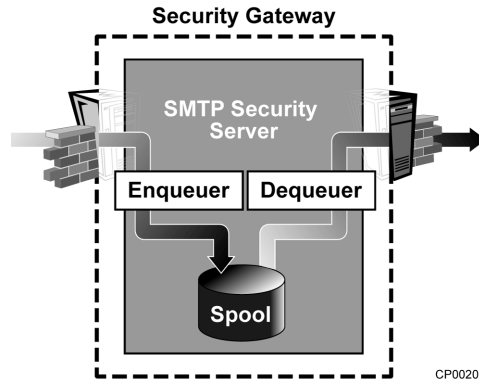
The SMTP protocol, designed to provide maximum connectivity among Internet users and enhanced to support file attachments, poses a challenge to Administrators who want to maintain connectivity and keep intruders out of their internal networks.

VPN-1 NGX offers an SMTP Security Server that provides highly granular control over SMTP connections. A new spool-dequeuer mechanism provides more efficient spool scanning by performing FIFO (first-in first-out), which enables mail to be put in the mail dequeuer, and prioritizes new mail over undeliverable old mail. The Administrator can:

- Hide outgoing mail's "from" address behind a standard generic address, which conceals internal network structure and real internal users.
- Perform mail filtering, based on SMTP and IP addresses.
- Strip MIME attachments from mail.
- Strip received information from outgoing mail, to conceal internal-network structure.
- Drop mail messages above a given size.
- Resolve DNS address for mail recipients and their domain on outgoing connections (MX resolving).
- Control the load generated by the mail dequeuer in two different ways:
 - By controlling the number of connections per site
 - By controlling the overall connections generated by the mail dequeuer
- Perform a mail-user based Policy, to:
 - Enable a mail-user based Policy.
 - Perform different mail actions per recipient of a given mail.
 - Enable the generation of different mail contents on a per-user basis.
 - Apply content-security features at the user level.
- Perform CVP checking.

Be aware that scanning settings may need to be adjusted to meet demand. For example, mail may be coming in faster than it can be scanned and sent to a mail server. To prevent this from happening, the default load settings must be changed manually.

The SMTP Security Server provides an additional layer of security over standard sendmail applications, by splitting functionality between two separate processes. This process ensures that no direct path connecting mail servers exists, preventing direct online connections to the real sendmail application protected by the Gateway.



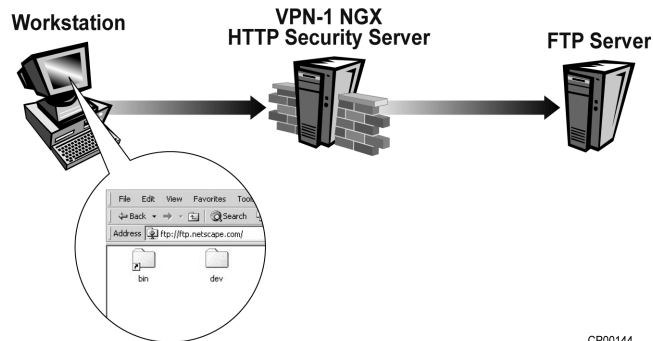
NGX SMTP Security Server

The above figure illustrates how one process, the enqueuer, writes incoming messages to a disk cache, and another process, the dequeuer, empties the cache.

FTP Security Server

The FTP Security Server provides authentication services and content security based on FTP commands (**PUT** and **GET**), file-name restrictions, and anti-virus checking for files. Implement an FTP Security Server with an FTP resource.

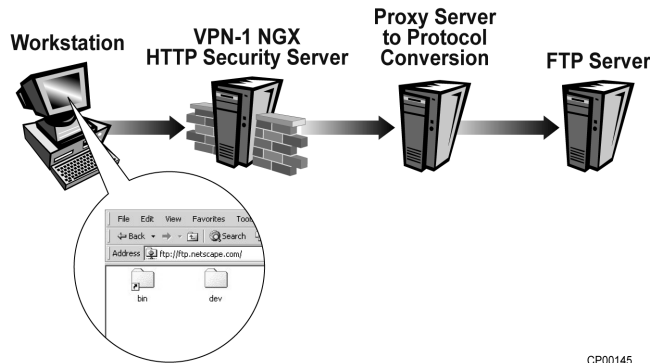
When using a browser without defining a proxy in the browser, all HTTP requests use the HTTP protocol, and all FTP requests use the FTP protocol. When using a browser with a proxy defined for FTP, the proxy defined should be an HTTP proxy, rather than an FTP proxy. When using this configuration, the connection between the browser and proxy uses the HTTP protocol. It is up to the proxy to convert the request from the HTTP protocol to the FTP protocol, as in this figure:



CP00144

NGX without Next Proxy Defined

The NGX HTTP Security Server does not support this kind of protocol conversion. Therefore, if you want to use VPN-1 NGX to authenticate FTP requests from a Web browser, a second HTTP proxy that does support this kind of protocol conversion should be installed and defined in SmartDashboard. Consider the configuration in this figure:



CP00145

VPN-1 NGX with Next Proxy Defined

If a next proxy is not defined on the Gateway and authentication is attempted for an FTP request, you will see the error message “scheme FTP not supported.”

Blocking FTP over HTTP for Specific Groups

To create a rule that would stop FTP over HTTP for certain groups, authentication needs to be used with a URI resource. The rule looks similar to this:

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	FTP Over HTTP Restriction Rule	All Users@Any	* Any	* Any Traffic	http->Kill_FTP-over_HTTP	Client Auth	Log

Block FTP over HTTP for Specific Groups Rule

1. In the URI resource that is used in this rule, use URI Match specification type Wild Card.
2. On the Match tab under Schemes, choose all desired schemes. Make sure FTP is cleared.

3. In the Host section, type *,*, indicating that HTTP is allowed out to any site and on any port. This will still allow users to connect to Web servers that use ports other than port 80.
4. In the Path and Query fields, * can be used.

This configuration will stop FTP via HTTP from passing through a Gateway.

Java and ActiveX Stripping

Administrators can control incoming Java and ActiveX code according to specific conditions, such as host, URL, or authenticated username. Capabilities of Java and ActiveX screening include the following:

- Stripping Java applet tags from HTML pages
- Blocking Java attacks, by blocking suspicious back connections
- Stripping ActiveX tags from HTML pages
- Implementing Java and ActiveX Stripping with a URI resource

CVP Inspection

CVP inspection is an integral component of VPN-1 NGX's content-security feature, and considerably reduces the vulnerability of protected hosts. CVP inspection examines all files transferred for all protocols. All NGX auditing tools are available for logging and alerting, when these files are encountered.

CVP inspection is implemented by Content Vectoring Servers. The interaction between VPN-1 NGX and the Content Vectoring Server is defined by Check Point's OPSEC framework. To implement CVP inspection:

1. Define a CVP OPSEC application. CVP OPSEC applications are defined in the CVP Group screen.
2. Define resource objects that specify CVP checking for the relevant protocols:

Use of CVP — Specify whether CVP is to be used.

CVP Server — If CVP is to be used, users must then define whether or not the CVP server is allowed to modify content, and whether or not to send HTTP headers to the CVP server.



CIFS resources do not invoke Security Servers, and the NGX Gateway does not broker the connection between server and client. Also, only a limited set of actions may be used for rules with CIFS resources. Only accept, client auth, and session auth may be used to populate the Action field of rules with a CIFS resource.

RESOURCES AND THE RULE BASE

NGX resources are only effective, if they are properly placed in the Rule Base of the Security Policy. If they are placed below generalized rules, the resource may never be used for its purpose. If the resource is not placed with appropriate follow-up rules, users may not be able to browse Web sites properly, or have the access they should be permitted.

Proper Rule Placement

To create a properly performing Rule Base, some general concepts are considered. The most commonly used rules should be placed at the top of the Rule Base. This allows the Gateway to efficiently analyze packets against the Rule Base. Most connections should be allowed or denied within the first few rules.

A pyramid-style construction is also useful. The more restrictive and specific rules should be placed at the top. The more generalized rules should be placed lower. This is a rule of thumb to keep in mind. It helps prevent an incorrectly configured Rule Base, allowing unwanted traffic to pass or restricting traffic that should pass.

Rules with resources should be located in the middle or beginning of a Rule Base, depending upon use. Restricted-access rules should go above resource rules, and generalized drop or accept rules should follow them. Below is a sample Rule Base with an HTTP resource rule:

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Net_Oslo	Any	Any Traffic	HTTP http->kill_FTP_over_HTTP	drop	Log	Policy Targets	Any	FTP Over HTTP Restriction Rule
2	Any	Any	Any Traffic	bootp NBT rip	drop	None	Policy Targets	Any	NetBIOS Rule
3	Any	fw.oslo.cp	Any Traffic	Any	drop	Log	Policy Targets	Any	Stealth Rule
4	www.madrid.cp	www.oslo.cp	Any Traffic	ftp telnet	accept	Log	Policy Targets	Any	Partner Cities Rule
5	Any	www.oslo.cp	Any Traffic	ftp	accept	Log	Policy Targets	Any	Web Server Rule
6	Net_Oslo	Any	Any Traffic	ftp	accept	Log	Policy Targets	Any	Web Traffic Rule
7	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Cleanup Rule

Rule Base Example

Consequences of Incorrectly Configured Rules

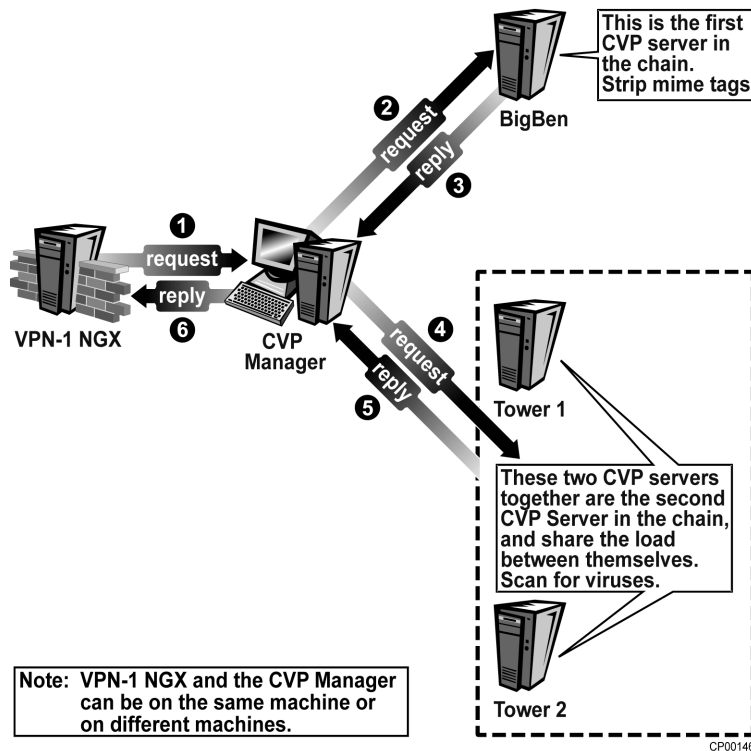
There are three possible outcomes when configuring resources in the Rule Base:

- Connections are allowed that should not be.
- Connections are dropped that should not be.
- The Security Server allows packets that should pass, and denies packets that should not pass.

The last condition is obviously the one desired by Administrators. The first two are typically due to rules that are placed in the incorrect order.

CVP LOAD SHARING AND CHAINING

VPN-1 NGX enables a resource to invoke any number of CVP servers. Identical CVP servers can be configured to share the load among themselves. This load-sharing capability increases efficiency.

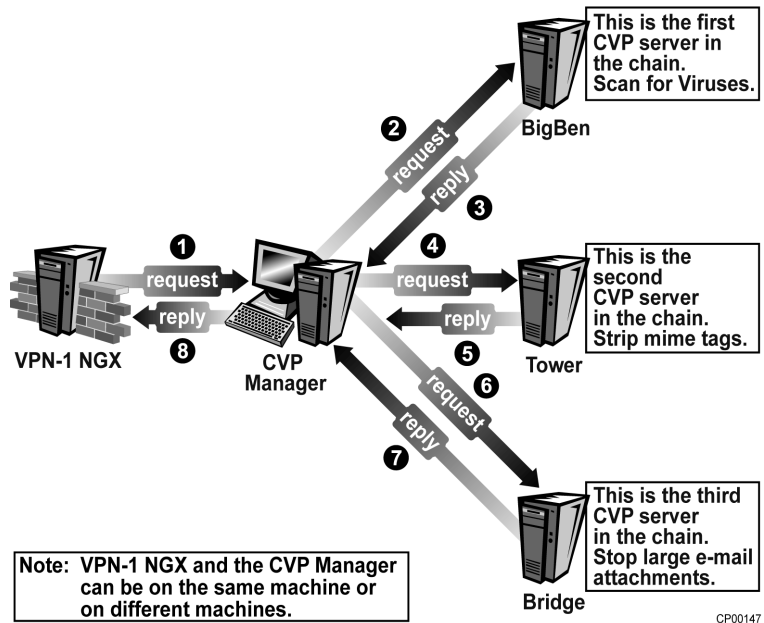


Three CVP Servers with Load Sharing



CVP Chaining

Chaining is useful when each of the CVP servers performs a different function. The chaining process connects servers for the purpose of stringing functionality. In the configuration shown below, the CVP Manager invokes the CVP servers on Bigben, Tower 1, and Tower 2, one after the other. Each CVP server has a different task, such as scanning for viruses, stripping MIME tags, or stopping large e-mail attachments.



Three CVP Servers in a Chain

IMPLEMENTING THE TCP RESOURCE

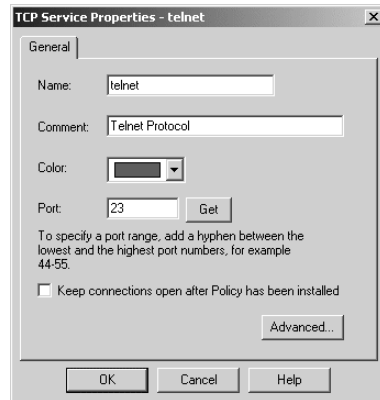
The TCP resource supports all TCP services. This resource allows URL screening via a UFP server, as well as providing CVP capabilities. If enabled, the UFP server can provide URL verification without using a Security Server. The full URL is not sent to the UFP server, only the IP address of the remote server. This allows faster transactions to occur, since name-to-IP resolution does not have to take place.



Before using the TCP resource, ensure the UFP server is capable of supporting IP-based URLs, and can categorize specific protocols that the TCP resource is going to be implementing.

Configuring TCP Security Servers

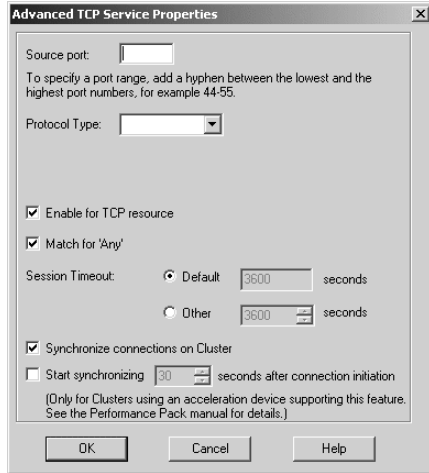
To enable the TCP resource, click the Advanced button in the TCP Service Properties screen:



TCP Service Properties Screen

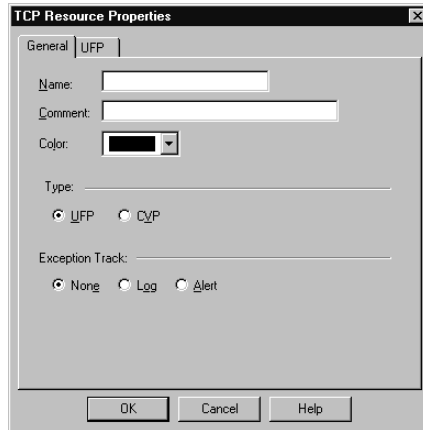


When Enable TCP for Resource is checked, the TCP resource is used for the Telnet service:



Enable for TCP Resource Checked

TCP Resource Properties



TCP Resource Properties Screen

Name — The resource's name

Comment — Descriptive text; this text is displayed on the bottom of the Resources screen, when this resource is selected.

Color — The color of the resource's icon; select the desired color from the drop-down list.

Type — The type of server to be used in the TCP resource:

UFP — When selected, a UFP server must be defined in the UFP tab.

CVP — When selected, a CVP server must be defined and CVP settings must be configured in the CVP tab.

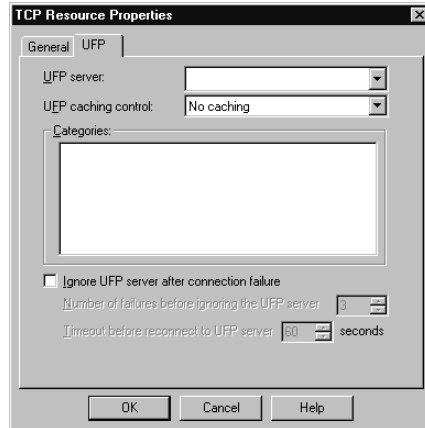
Exception Track — Determines if an action (specified in the Action tab) taken as a result of a resource definition is logged; select one of the following:

None — No logging or alerting

Log — An event logged

Alert — An alert issued

UFP Tab



UFP Tab

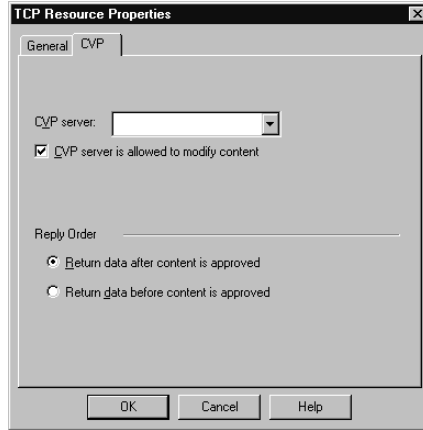
UFP server — The UFP server’s name, as selected from the drop-down list; the UFP server maintains a list of URLs and their categories. VPN-1 NGX checks connection attempts, using the URL list on the UFP server. When a user requests a URL, VPN-1 NGX determines if the UFP server must be used, and handles the request without using a Security Server. If the UFP server is used, the connection packet is temporarily held, until VPN-1 NGX determines if the connection is permitted.

UFP caching control — Specifies how caching is to be enabled; the Administrator can select No caching, Caching on the UFP server, or Caching 1 or 2 requests on VPN-1 NGX.

Categories — The categories you wish to include in the resource definition

Ignore UFP server after connection failure — Allows Administrators to determine the length of time before the Gateway ignores a UFP server; this may be used in case of failure of the UFP server to allow traffic to pass. A time-out is also set to allow the Gateway to attempt a reconnection. During the time the NGX Gateway is ignoring the UFP server, traffic is not being scanned.

CVP Tab



CVP Tab

In the CVP tab of the TCP Resource Properties screen, define the following:

CVP Server — The name of the CVP server

CVP Server is allowed to modify content — Allows the CVP server to modify content of the message string

Reply Order — Designates when data is to be returned to users; you must select one of the following:

- Return data after content is approved
- Return data before content is approved