CISCO SYSTEMS

Doc. No.

Upgrading Centri Firewall 3.1x to Cisco Centri Firewall 4.0

Before You Begin

Understanding the Document Scope

This document guides you through the process of upgrading your existing Centri Firewall 3.1x product to Cisco Centri Firewall 4.0. It includes information relevant only to upgrading the firewall product; therefore, discussions concerning peripheral concerns, such as upgrading to Windows NT 4.0 or converting DNS from MetaInfo to Microsoft DNS, are not included. Please refer to other sources for information about those peripheral concerns. We also assume that you have read and understand the documentation accompanying Cisco Centri Firewall 4.0, so we do not duplicate discussions relating to creation of security policies or network objects.

Getting Help

You should contact your reseller if you have questions about Centri Firewall 3.1x or the upgrade process to Cisco Centri Firewall 4.0.

Existing Support Contracts

Existing support contracts for Centri Firewall 3.1x will end July 15, 1998. You should contact your reseller if you have questions about your existing support contract.

Upgrading the Windows NT Operating System

Cisco Centri Firewall 4.0 does not run on the Windows NT 3.51 operating system. Therefore, you need to upgrade your operating system to Windows NT 4.0 with the service pack included with Cisco Centri Firewall 4.0.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

However, before you perform this upgrade, you should complete Worksheet A. Then, you should perform a system-wide backup and remove Centri Firewall 3.1x and MetaInfo DNS.

Concerning DNS

MetaInfo DNS, which shipped with Centri Firewall 3.1x, does not accompany Cisco Centri Firewall 4.0 (and does not run on Windows NT 4.0); however, it is not required for firewall functionality. However, if you would like to continue running DNS on your firewall, we suggest using the Microsoft DNS server that ships with Windows NT Server 4.0. Please refer to Microsoft documentation for information concerning use of that product.

Firewall Architecture

Centri Firewall 3.1x

Centri Firewall 3.1x is a firewall that operates by comparing a requested service with two tables: one listing denied IP addresses and another listing allowed IP addresses. To construct a security rule in Centri Firewall 3.1x, you assign IP addresses to services. With Centri Firewall 3.1x, an administrator views a network as a combination of independent IP addresses without an inherent hierarchy.

Centri Firewall 3.1x performs automatic Network Address Translation (NAT) for proxy-based services. It also supports packet-filtering capabilities and has a concept of a plug/proxy service. SNK authentication, HTTP caching, and TCP/UDP port ranges are additional features of Centri Firewall 3.1x.

Cisco Centri Firewall 4.0

Cisco Centri Firewall 4.0 is a firewall that operates by comparing a network object initiating a service request with the security policy attached to or inherited by that network object. The process of creating an attached security policy comprises several steps: first, you need to assign the network object a place within the network hierarchy; then, you need to construct with the graphical policy-construction tool a security policy that permits services through the firewall; finally, you need to attach that new policy (or an existing policy) to the network object via a “drag-and-drop” operation. Essentially, with Cisco Centri Firewall 4.0, an administrator views a network as a combination of network objects organized into a meaningful hierarchy. The administrator either can apply a security policy to an individual network object or can apply the security policy to the larger organizational structure of which that individual network object is a member.

Cisco Centri Firewall 4.0 supports NAT for all services, although NAT must be manually configured. However, because of the technological advance of the Kernel Proxy architecture, packet-filtering has become obsolete, and the plug/proxy service has been replaced by a combination of exposed services and network objects. SNK authentication, HTTP caching, and TCP/UDP port ranges are not features of Cisco Centri Firewall 4.0.

Upgrade Procedures

Before Removing Centri Firewall 3.1x

Before you remove Centri Firewall 3.1x, you should obtain information about the following: IP addresses of your firewall, persistent routes, plug/proxy servers (if any), and internal mail server (if any). The following sections walk you through the processes involved in obtaining that information and provides you with a worksheet on which to record it.

Finding Firewall IP Addresses

Using the command **ipconfig** at the command prompt displays the network adapter name, IP address, subnet mask, and default gateway. Record this information in Worksheet A.

Finding Persistent Routes

Using the command **route -p print** at the command prompt displays two lists: the first list includes your active routes, while the second list includes your persistent routes. Remember that not all systems have persistent routes. If the **route -p print** command displays information in the second list, record the network address, netmask, gateway address, and metric for each entry in Worksheet B.

Finding Plug/Proxy Servers

Within the Centri Firewall 3.1x graphical interface, go to the Plug/News node and click the Servers tab. For each entry, record the IP address listed under To IP address in the Hidden Address field of Worksheet C; record the port number listed under To port as a numerical value (service names such as SMTP are not allowed) in the Hidden Port field of Worksheet C; record the IP address for the outside interface of the firewall in the Exposed Address field of Worksheet C; and record the port number listed under From port as a numerical value (service names such as SMTP are not allowed) in the Exposed Port field of Worksheet C.

Finding Your Internal Mail Server

Within the Centri Firewall 3.1x graphical interface, go to the SMTP node, and if you find an entry for an Internal Mail Host, do the following: for an IP address entry, record that data in the Hidden Address field of Worksheet C; for a DNS name, at the command prompt use **nslookup hostname** to find this IP address and then record the resultant data in the Hidden Address field of Worksheet C.

To complete the entry for your internal mail server, record the value 25 in the Hidden Port and Exposed Port fields of Worksheet C, and also record the IP address for the outside interface of the firewall in the Exposed Address field of Worksheet C.

Worksheet A

Adapter Name	IP Address	Subnet Mask	Default Gateway

Worksheet B

Network Address	Network Mask	Gateway Address	Metric

Worksheet C

Hidden Address	Hidden Port	Exposed Address	Exposed Port

Installing Cisco Centri Firewall 4.0

Refer to the *Cisco Centri Firewall Installation Guide* for detailed information about how to install the firewall. Use the information that you recorded in Worksheet A to configure adapter card IP addresses and the default gateway during the installation process.

Configuring Routing

If your Centri Firewall 3.1x configuration did not include persistent routes (refer to Worksheet B), your routing should already be configured properly. However, if that previous configuration included persistent routes, then you need to follow these steps in order to configure your routing properly:

Step 1 In the Navigation pane of Centri Administrator, expand the Networks tree and double-click the CentriFirewall node.

Step 2 Click the Routes tab.

Step 3 For each route, type the appropriate information for network address, network mask, gateway address, and metric in the respective fields (refer to Worksheet B), then click **Add**.

Step 4 When you are finishing with all routing information, click **OK** to accept the changes.

Step 5 To ensure that these changes take effect, save the Centri Administrator portion of the Security Knowledge Base by clicking the File menu, pointing to Centri Administrator, and clicking **Save**.

Configuring Exposed Services

Exposed services are the Cisco Centri Firewall 4.0 equivalent of plug/proxy services and internal e-mail delivery. If you do not need to expose any services, then proceed to the next section.

Step 1 In the Navigation pane of Centri Administrator, expand the Networks tree and double-click the CentriFirewall node.

Step 2 Click the Exposed Services tab.

Step 3 For each service, type the appropriate information for name, description, type (UDP or TCP), exposed address, exposed port, hidden address, and hidden port in the respective fields (refer to Worksheet C), then click **Add**.

Step 4 When you are finished adding all exposed services information, click **OK** to accept the changes.

Step 5 Note that for each exposed service, a security policy that allows this service must be attached to the network object from which you expect a request for the exposed service to originate (refer to Cisco Centri Firewall 4.0 documentation for help). For example, if you want to allow inbound e-mail traffic from the Internet, you must attach a policy allowing the SMTP service to the Internet network object located in the Networks tree.

Step 6 To ensure that these changes take effect, save the Centri Administrator portion of the Security Knowledge Base by clicking the File menu, pointing to Centri Administrator, and clicking **Save**.

Converting Rules to Attached Security Policies

This section attempts to help you convert the security rules developed in Centri Firewall 3.1x to security policies that can be attached to network objects in Cisco Centri Firewall 4.0. While focusing on the major issues common to all network setups, we cannot foresee or discuss all the possibilities in securing a network. Therefore, we present three different scenarios, one or more of which should guide you through the process of converting your security rules to functional security policies. The examples included with these scenarios are oversimplified for purposes of clarity.

The first scenario involves a situation in which your access rules are based on entire networks. In other words, if your rule sets within Centri Firewall 3.1x include permissions universal to individual networks, then you can create network objects within Cisco Centri Firewall 4.0 and attach security policies to them.

For example, if all of your rule sets within Centri Firewall 3.1x include 192.168.1.*, you can create a trusted physical network (named Network A) within Cisco Centri Firewall 4.0 with an IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 (see “Understanding the Use of “*” in Network Addresses” for a brief discussion on converting networks with “*” symbols to network/netmask pairs). Then you can define a security policy in Cisco Centri Firewall 4.0 that allows the network services defined within those previous rule sets. Attaching the security policy to the trusted physical network enables the security policy for that network object, in this case, Network A.

Here is an even more specific example. If your only rule set within Centri Firewall 3.1x is to allow Telnet services for the IP addresses 192.168.1.*, then you can create a security policy within Cisco Centri Firewall 4.0 that allows Telnet and attach it to a network object, in this case Network A, defined as a trusted physical network with an IP address of 192.168.1.0 and a subnet mask of 255.255.255.0.

The second scenario involves a situation similar to the first, but you have also included exceptions to your rule sets in which access to services is denied. In other words, if your rule sets within Centri Firewall 3.1x contain denial entries for one or more proxies, then you need to create independent network objects within Cisco Centri Firewall 4.0 for those exceptions and attach security policies to those individual network objects.

For example, if your only rule set within Centri Firewall 3.1x is to allow Telnet services for IP addresses 192.168.1.* with the exception of 192.168.1.4 (specified in the deny list for the Telnet proxy), then you can create a security policy within Cisco Centri Firewall 4.0 that allows Telnet and attach it to a network object, in this case Network A, defined as a trusted physical network with an

IP address of 192.168.1.0 and a subnet mask of 255.255.255.0. Furthermore, you can create a trusted host with an IP address of 192.168.1.4 within Cisco Centri Firewall 4.0 and attach another security policy that denies Telnet services to that trusted host.

The third scenario involves a situation much different from the first two in that your rule sets within Centri Firewall 3.1x comprise individual hosts rather than networks. In other words, if your rule sets within Centri Firewall 3.1x contain individual IP addresses, then you can create trusted host network objects within Cisco Centri Firewall 4.0 and attach security policies to them.

For example, if your only rule set within Centri Firewall 3.1x is to allow Telnet for the host 192.168.1.4, then you can create a trusted host network object within Cisco Centri Firewall 4.0 with the IP address 192.168.1.4 and attach a security policy allowing Telnet services to that trusted host.

Understanding the Use of "*" in Network Addresses

In Centri Firewall 3.1x, the use of "*" is commonly used to signify a range of computers. Cisco Centri Firewall 4.0, however, does not use this convention but instead uses the combination of a network IP address and a subnetwork mask. If you need to convert simple IP ranges to the system used by Cisco Centri Firewall 4.0, follow the directions in the table in "Converting IP Ranges to Network Addresses."

Converting IP Ranges to Network Addresses

IP Range	Network	Subnet Mask
X.Y.Z.*	X.Y.Z.0	255.255.255.0
X.Y.*.*	X.Y.0.0	255.255.0.0
X.*.*.*	X.0.0.0	255.0.0.0
..*.*	0.0.0.0	0.0.0.0

This document is to be used in conjunction with the *Cisco Centri Firewall Installation Guide* publication.

977R