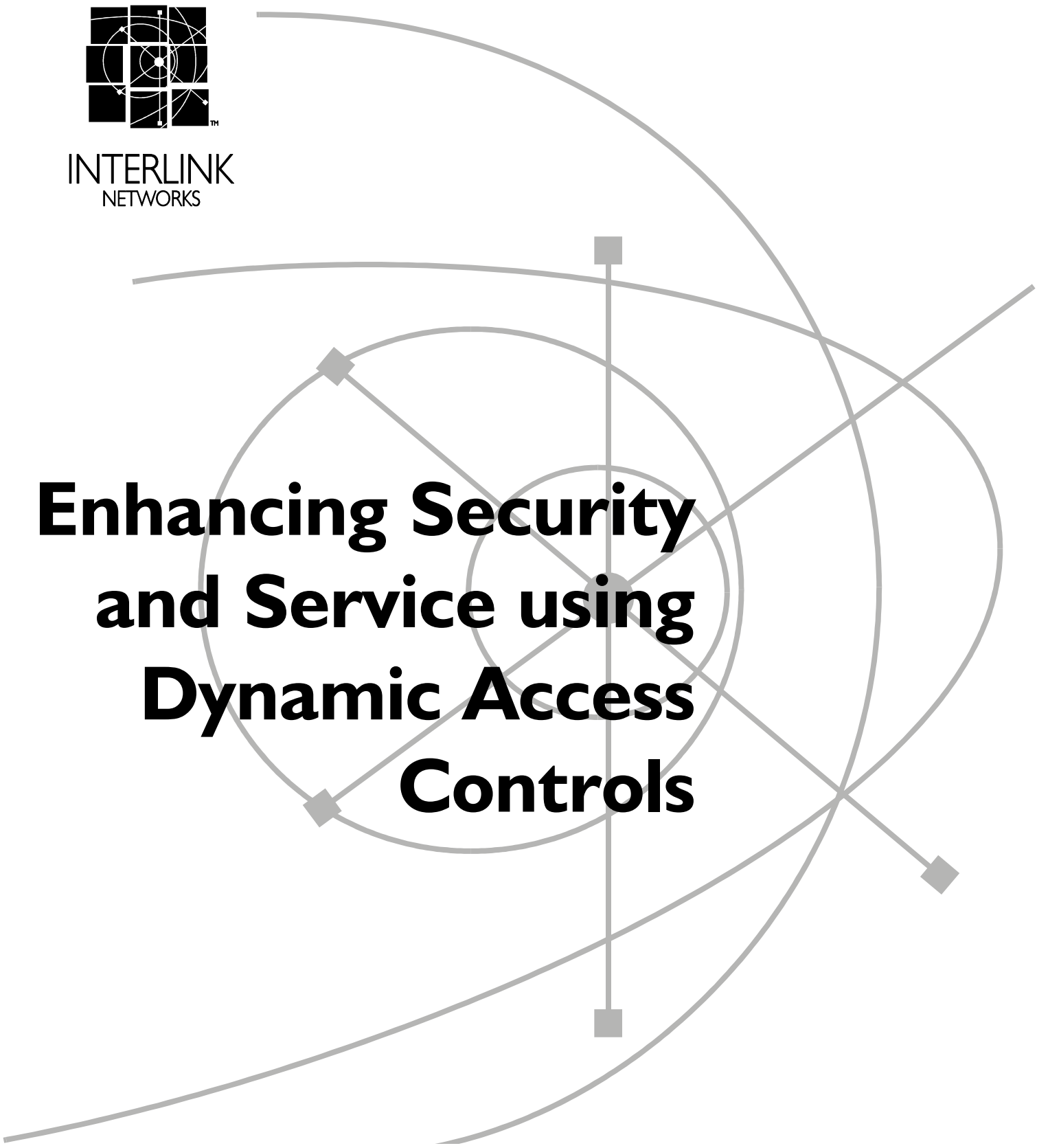

Enhancing Security and Service using Dynamic Access Controls

Revision **A**

Interlink Networks, Inc.

775 Technology Drive, Suite 200
Ann Arbor, MI 48108 USA
Phone: 734-821-1200
Sales: 734-821-1228
Fax: 734-821-1235
info@interlinknetworks.com
sales@interlinknetworks.com
www.interlinknetworks.com

Enhancing Security and Service using Dynamic Access Controls

Business, like life, is filled with rules. Business rules are documented and implemented as policies. Policies can protect company resources, define services, and make the delivery of those services consistent and of high quality. Policies can be fixed and constant, or they can be dynamic and vary over time.

DYNAMIC POLICY OVERVIEW

We come in contact with dynamic policies every day. A bank vault that can only be opened during certain hours is an implementation of a dynamic policy to increase security. Lowering the speed limit in a school zone during school hours is a dynamic policy that changes service levels rather than denying service. Lower ticket prices for matinee movies is a dynamic policy that does not limit service but accounts for it differently based on the time the service is delivered. These simple real life examples illustrate that policies are powerful tools for delivering value in various ways to customer and company alike.

SOLUTION

Interlink Networks has made it possible to implement powerful dynamic access controls with the introduction of new attributes based on the system clock of the server. The RAD-Series line of RADIUS servers generates the following Interlink Networks attributes for every Access-Request:

- `Day-Of-Week` (syntax is a 3 character day, e.g. Sun, Mon, etc.)
- `Date-Time` (syntax is yyyy:mm:dd:hh:mm, e.g. 2001:12:25:06:00)
- `Time-of-Day` (syntax is hh:mm, e.g. 17:00)

The Interlink Networks dynamic access control attributes are generated specifically for use in policies internal to the RAD-Series server. The attributes are not forwarded in proxy RADIUS requests nor are they transmitted to the NAS in RADIUS responses. It should

also be noted that the dates and times recorded in the attributes are those of the Interlink Networks RADIUS server platform, not those of the NAS or any other network element.

These attributes can be used with any of the RAD-Series server's various policy engines to write powerful dynamic access controls. Interlink Networks dynamic access controls are most powerful when used with either Interlink Networks ProLDAP or the Interlink Networks Advanced Policy Engine. These tools offer a wide range of evaluators and Boolean operators for defining policies.

EXAMPLE – ACCESS LIMITED TO WEEKDAYS

TGIF Company has a company-wide policy that its employees can only access company resources during weekdays. TGIF has implemented this using simple policy in the form of Deny-Items in the RAD-Series users file.

```
DEFAULT Authentication-Type = Realm, Day-Of-Week != Sun, Day-Of-Week !=
Sat
```

In this policy, the Day-Of-Week may NOT equal either Sun or Sat or access is denied.

EXAMPLE – ACCOUNT EXPIRATION

The Techno School District provides filtered Internet access to its students during the school year for research and academic projects. All of the students have User-Ids in the student.techno.edu realm. The student accounts expire at the end of the last day of school. The account expiration policy is enforced using a decision file and the Interlink Networks Advanced Policy Engine.

```
Group Student-Accounts {
            Condition  {
                  (User-Realm = student.techno.edu) &&
                  (Date-Time > 2002:06:11:15:30)
            }
            Reply {
                  Decision = NAK
                  Reply-Message = "Your student account has expired."
            }
}
Group Staff-Accounts   {
            Reply {
                  Decision = ACK
```

```
            }
}
```

This policy uses the RAD-Series User-Realm VSA (vendor-specific attribute) to identify student accounts and deny their access after the end of school Date-Time. All other accounts for school district staff are in a different realm and do not have the dynamic access control policy applied.

EXAMPLE – TIME BASED SERVICE LIMITS

BigISP has two service levels it sells to its subscribers. It has a premium service it sells to businesses that provides unlimited access. It sells a lower priced service to individuals that limits sessions to 30 minutes during primetime business hours but allows unlimited access outside of business hours. BigISP has defined primetime business hours to be 8:00 am to 6:00 pm Monday through Friday. BigISP has created its own VSA, Acct-Type, where customer service maintains the service level purchased, either Premium or Standard. The two levels of service are implemented using a decision file and the Interlink Networks Advanced Policy Engine.

```
Group Premium     {
            Condition   {
                  Acct-Type = Premium
            }
            Reply {
                  Decision = ACK
            }
}
Group Standard-Primetime     {
            Condition   {
                  (Acct-Type = Standard) &&
                  (Day-Of-Week >= Mon) &&
                  (Day-Of-Week <= Fri) &&
                  (Time-Of-Day >= 08:00) &&
                  (Time-Of-Day <= 18:00)
            }
            Reply {
                  Decision = ACK
                  Session-Timeout = 1800
            }
}
```

```
Group Standard-Offhours      {
            Condition   {
                  Acct-Type = Standard
            }
            Reply {
                  Decision = ACK
            }
}
Group Invalid-Account   {
            Reply {
                  Decision = NAK
            }
}
```

BigISP's policy recognizes four groups of policies and checks them in sequence until it finds one that applies. If the account is a Premium account, then access is granted. If the access request comes during the primetime period and the account is a Standard account, then access is limited to thirty minutes. If the account is Standard and did not get caught by the primetime check, then access is granted without limit. Finally, if the request did not meet any of the prior conditions, then the request is invalid and access is denied.

SUMMARY

The dynamic access controls implemented with the Interlink Networks RAD-Series line of RADIUS servers are powerful tools for increasing security, defining services, managing resources, and delivering quality service to both the enterprise and the end user.

ABOUT INTERLINK NETWORKS

THE COMPANY

Interlink Networks is a leader in securing access to public and private networks. Our products manage user access to dial-in, broadband, mobile, and wireless LAN networks. Interlink Networks' RADIUS-based access control software provides the authentication, authorization, and accounting infrastructure that enables secure and reliable network access for thousands of enterprise and service provider networks worldwide.

Interlink Networks is headquartered in Ann Arbor, Michigan. We have a worldwide network of resellers and distributors.

OUR MISSION

Interlink Networks' mission is to be a worldwide leader in providing solutions for securing access to public and private networks. By securing access to the network, we provide network operators the first line of defense against unauthorized access to an organization's computing resources.

OUR HISTORY

In July 2000, Interlink Networks was formed by a spin out of technology and developers from Merit Network, Inc., a world-renowned designer, developer, and implementer of Internet technology, hosted at the University of Michigan.

The founders of Interlink Networks spent over a decade defining and developing the world's best carrier-class RADIUS (Remote Access Dial-In User Services) server. Mr. John Vollbrecht, Interlink Networks' Founder and CTO, issued the first RFP for centralized AAA ten years ago, and championed the resulting RADIUS standards through the IETF Standards Groups. Mr. Vollbrecht's name is on many of the RFCs that define RADIUS and AAA.

The charter of Interlink Networks is to expand upon its vision of providing the most advanced authentication products, and to expand its solution set beyond remote access into other network access mechanisms that require authentication and authorization. As networks become more complex, and the means to access networks expands, Interlink will continue to assure that the "interlinks" between users and their networks are protected and secure.